SpruceID

Spruce Systems, Inc.
228 Park Ave S, PMB 28788
New York, New York 10003-1502 US

July 30, 2026

The Honorable Mehmet Oz, M.D.
Administrator
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244

Submitted electronically via https://www.regulations.gov (Docket No. CMS-2026-2047)

Re: CMS-2454-IFC, Medicaid Program; Community Engagement Requirement for Certain Individuals, Interim Final Rule with Comment Period, 91 FR 33348 (June 3, 2026)

Dear Administrator Oz,

Spruce Systems, Inc. (dba SpruceID) appreciates the opportunity to comment on the interim final rule implementing the Medicaid community engagement requirement. SpruceID designs and operates standards-based digital identity, credentialing, verification, and secure data exchange infrastructure for government programs. Our work includes supporting the California Department of Motor Vehicles' mobile driver's license program,[1] the State of Utah's verifiable digital credential program,[2] and the National Institute of Standards and Technology's National Cybersecurity Center of Excellence work on mobile driver's licenses and verifiable digital credentials.[3] Our comments draw on that experience and focus specifically on how states can verify qualifying activities and exemptions while reducing administrative burden and erroneous coverage loss.

SpruceID does not address the merits of the statutory community engagement requirement. Our comments focus on its implementation, particularly how states can verify compliance and exemptions without creating avoidable procedural barriers for eligible individuals. The rule requires states to establish significant new verification and documentation processes on an accelerated timeline. The design of those processes will affect administrative cost, program integrity, beneficiary burden, and the risk that eligible individuals lose coverage because required information cannot be located or submitted.

We recommend that CMS take the following actions through regulatory clarification, subregulatory guidance, grant conditions, and voluntary state pilots, as appropriate:

[1] California DMV, mDL Adoption Statistics: https://www.dmv.ca.gov/portal/mdl-adoption-statistics/
[2] Utah Division of Technology Services, Verifiable Digital Credentials: https://dts.utah.gov/what-we-are-doing/our-initiatives/verifiable-digital-credentials/
[3] NIST NCCoE, Digital Identities: Mobile Driver's License: https://www.nccoe.nist.gov/projects/digital-identities-mdl

1. Maximize ex parte verification, automatically apply supported exemptions, and preserve self-attestation where documentation is not reasonably available.
2. Recognize pre-authorized, consent-based data sharing as ex parte verification.
3. Recognize standards-based verifiable digital credentials as an optional form of beneficiary-submitted evidence.
4. Permit authorized providers and agencies to issue reusable exemption attestations.
5. Support optional cross-program status attestations where program rules align.
6. Permit federal modernization funding to support interoperable evidence exchange.
7. Establish voluntary state pilots before the 2028 documentation transition.
8. Apply proportionate identity assurance without mandating a particular provider, application, or biometric method.

These recommendations are intended to expand the ways individuals may establish compliance or exemption status, not replace existing processes. Digital credential pathways should remain voluntary and should supplement paper, telephone, in-person, and caseworker-assisted options. Medicaid eligibility should not depend on smartphone ownership, use of a particular application or vendor, or completion of biometric identity verification.

I. Verification design will materially affect coverage outcomes

Recent Medicaid eligibility experience demonstrates that procedural failures can cause substantial coverage loss even when an agency has not determined that the affected individuals are ineligible. During the unwinding of the continuous enrollment provision, more than 25 million people were disenrolled, and approximately 69 percent of those disenrollments were classified as procedural.[4] Ex parte renewal rates also varied substantially among states,[5] indicating that differences in data access, system design, and administrative practice can materially affect whether eligible individuals retain coverage.

Arkansas's 2018 work requirement provides the closest prior implementation example. More than 18,000 adults lost coverage for failure to meet reporting requirements in less than one year.[6] Subsequent research found that more than 95 percent of the target population appeared either to satisfy the requirement or qualify for an exemption, while confusion and limited awareness of the

[4] KFF, As Medicaid Unwinding Concludes in Most States, KFF Finds 25 Million Lost Medicaid Coverage…: https://www.kff.org/medicaid/as-medicaid-unwinding-concludes-in-most-states-kff-finds-25-million-lost-medicaid-coverage-but-enrollment-is-10-million-higher-than-pre-pandemic-levels/
[5] KFF, Understanding Medicaid Ex Parte Renewals During the Unwinding: https://www.kff.org/medicaid/understanding-medicaid-ex-parte-renewals-during-the-unwinding/
[6] KFF, State Data for Medicaid Work Requirements in Arkansas: https://www.kff.org/medicaid/issue-brief/state-data-for-medicaid-work-requirements-in-arkansas/

reporting process were common.[7] Georgia's Pathways program presents a related cost concern: the GAO reported $54.2 million in administrative expenditures compared with $26.1 million in health care benefit expenditures during the period examined.[8] Together, these experiences indicate that documentation-intensive processes can impose high administrative costs while failing to distinguish reliably between ineligible individuals and eligible individuals who encounter reporting barriers.

The scale of implementation under this rule is significantly larger. Forty-three states must implement the requirement, and roughly 20 million expansion enrollees may be subject to it.[9] The rule appropriately requires states to attempt ex parte verification using information already available before requesting documentation from the individual. However, states estimate that data matching may verify compliance or exemption for only 60 to 80 percent of affected enrollees.[10] The remaining population is likely to include individuals whose income or work activity is not consistently represented in conventional payroll data, including self-employed, seasonal, gig, cash-economy, and multiple-employer workers.

The transition after December 31, 2027, warrants particular attention. During the initial implementation period, states may accept self-attestation under penalty of perjury when reliable electronic data is unavailable. Beginning January 1, 2028, states generally must require documentation when it is reasonably available.[11] For individuals whose compliance or exemption cannot be established through existing data sources, this change may shift a substantial evidentiary burden to the beneficiary. The Arkansas experience demonstrates the risk of coverage loss when documentation processes are difficult to understand or complete. The recommendations below are intended to reduce that risk while preserving appropriate verification and program-integrity controls.

II. Recommendations

Recommendation 1: Strengthen data-first verification and automatic exemption processing

CMS should direct and support states to maximize ex parte verification so that most enrollees do not receive a documentation request. Where reliable state or federal data establishes that an individual

[7] New England Journal of Medicine, Medicaid Work Requirements—Results from the First Year in Arkansas: https://www.nejm.org/doi/full/10.1056/NEJMsr1901772
[8] GAO report on Georgia Pathways. Existing copy: https://www.warnock.senate.gov/wp-content/uploads/2025/09/GAO-GA-Pathways-Report.pdf
[9] KFF, An Early Look at Policy Decisions as States Get Ready to Implement Work Requirements: https://www.kff.org/medicaid/an-early-look-at-policy-decisions-as-states-get-ready-to-implement-work-requirements/
[10] KFF, An Early Look at Policy Decisions as States Get Ready to Implement Work Requirements: https://www.kff.org/medicaid/an-early-look-at-policy-decisions-as-states-get-ready-to-implement-work-requirements/
[11] State Health and Value Strategies, CMS Releases Interim Final Rule on Medicaid Work Reporting Requirements: https://shvs.org/cms-releases-interim-final-rule-on-medicaid-work-reporting-requirements/

qualifies for a mandatory exemption, the state should apply that exemption without requiring a separate application or duplicative submission. CMS should also consider extending the period during which states may rely on self-attestation when reliable electronic data is unavailable, or clarify that documentation is not "reasonably available" when obtaining it would impose a disproportionate burden or create a foreseeable risk of erroneous termination.

Ex parte verification should remain the primary mechanism because it reduces beneficiary burden and eligibility-worker workload.[12] Code for America's work with Minnesota expanded ex parte consideration to approximately 70 percent of a caseload previously renewed manually and reduced worker time per renewal from approximately 70 minutes to 15 minutes.[13] The statute also permits states to elect not to require individual verification of mandatory exemptions.[14] Beneficiary-held evidence should therefore serve as an additional pathway for cases that cannot be resolved through authoritative data, not as a substitute for improving state verification systems.

Recommendation 2: Recognize pre-authorized data sharing as ex parte verification

Credential pathways that are pre-authorized by the individual and directly available to the consuming agency without further user action should be treated as ex parte verification, because the determination is completed without any action by the individual at the time of the review, and the agency is able to verify the information's authenticity. CMS should confirm in subregulatory guidance that states may rely on these pre-authorized pathways as reliable electronic information in the data-first verification process. For example, under an appropriate privacy framework, an individual may authorize a ride-sharing platform, a peer-to-peer tasking platform, or a data wallet service that collects verifiable digital credentials from such platforms, to share a limited set of data automatically with a specific state agency for the purpose of eligibility determination only.

This is consistent with the consent-based approach CMS has taken in its Eligibility Made Easy income verification tool. The individual may revoke the authorization at any time; revocation should route the individual to another verification pathway and should not be treated as evidence of noncompliance. In this arrangement the information is directly available to the agency, and the digital signature allows the agency to verify its source and integrity.

---

[12] Pamela Herd, Eric R. Giannella, Jeremy Barofsky, Luke Farrell, and Donald Moynihan, "Interventions to Automate Medicaid Renewals Reduce Procedural Denials and Increase Coverage," Health Affairs, Vol. 44, No. 11, November 3, 2025, https://doi.org/10.1377/hlthaff.2025.00316.
[13] Code for America, "Building Human-Centered Benefits Renewal Processes with Client Equity in Mind," https://codeforamerica.org/news/human-centered-ex-parte-benefits-renewals/.
[14] Center on Budget and Policy Priorities, "A Guide to Reducing Coverage Losses Through Effective Implementation of Medicaid's New Work Requirement," https://www.cbpp.org/research/health/a-guide-to-reducing-coverage-losses-through-effective-implementation-of-medicaids.

Spruce Systems, Inc.
228 Park Ave S, PMB 28788
New York, New York 10003-1502 US

Consistent with the minimization principle in NIST SP 800-53 SA-8(33), CMS should require use of data minimization for any credential-based pathway and protection of user privacy and consent, regardless of whether the data are requested directly from the user or from another system. States should request, receive, and retain only the attributes necessary for the eligibility determination and applicable audit requirements. Systems should not retain complete credentials, transaction histories, device identifiers, or unrelated underlying records when a narrower verification result is sufficient.

Recommendation 3: Recognize standards-based verifiable digital credentials as an optional form of beneficiary-submitted evidence

CMS should clarify in subregulatory guidance that states may accept a standards-based verifiable digital credential, presented directly by the individual, as evidence of a qualifying activity, income amount, or exemption when the credential is issued by an authorized source and contains the information necessary for the eligibility determination. After 2027, such a credential should be accepted as one permissible form of beneficiary-submitted documentation. Use of this pathway should remain voluntary.

A verifiable digital credential is a digitally signed record issued by an entity such as an employer, payroll provider, educational institution, community service organization, health care provider, or government agency. The digital signature allows a receiving system to verify the credential's issuer and confirm that the information has not been altered. CMS and states would still need to define which issuers are authorized to attest to particular facts, which data elements are accepted, and how credential expiration, revocation, and audit requirements are handled.

Within an appropriate trust framework, credentials can reduce repetitive documentation while allowing the individual to control when evidence is presented. The individual may reuse current evidence across verification cycles and disclose only the information required for the determination. CMS should specify open, nonproprietary standards for issuance and presentation so that states may use multiple conforming products or build components themselves without dependence on a single vendor.

A credential validation failure should not, by itself, support denial or termination. If a credential cannot be validated because of technical unavailability, expiration, issuer-status uncertainty, or format incompatibility, the state should notify the individual and provide a reasonable opportunity to use another verification pathway. CMS should require states to distinguish an affirmative determination of noncompliance from an inability to complete electronic validation.

Spruce Systems, Inc.
228 Park Ave S, PMB 28788
New York, New York 10003-1502 US

Recommendation 4: Permit authorized provider and agency attestations of exemption status

CMS should permit states to accept, at the individual's election, a verifiable digital credential issued by an authorized health care provider, government agency, or other approved source attesting that the individual qualifies for a specified exemption. The credential should identify the applicable exemption category, validity period, issuer, and expiration or review date without requiring disclosure of underlying clinical or personal information that is not necessary for the eligibility determination.

This approach would be particularly valuable for conditions or circumstances that remain valid across multiple eligibility reviews. It would allow an individual to reuse a current attestation rather than repeatedly requesting equivalent documentation from a provider or agency. CMS should distinguish permanent or long-term exemptions from time-limited exemptions, such as pregnancy or temporary medical circumstances, and establish validity and renewal rules appropriate to each category.

Recommendation 5: Support opt-in cross-program status attestations where program rules align

Because compliance with certain SNAP or TANF work requirements may establish an exemption from the Medicaid community engagement requirement,[15] CMS should coordinate with the Food and Nutrition Service and the Administration for Children and Families to define a common, optional status attestation.[16] A participating agency could issue a signed credential indicating that, for a defined period, an individual has been determined to satisfy or be exempt from a specified requirement.

A beneficiary could elect to present that attestation to another participating program or state, which would evaluate it under the receiving program's applicable rules. This would not require automatic acceptance where legal standards differ, but it could eliminate duplicative collection when an existing determination is sufficient. A beneficiary-mediated approach may also reduce the need for each pair of agencies to establish a new point-to-point data exchange while leaving existing interagency data-sharing processes unchanged.[17]

---

[15] State Health and Value Strategies, "CMS Releases Interim Final Rule on Medicaid Work Reporting Requirements," https://shvs.org/cms-releases-interim-final-rule-on-medicaid-work-reporting-requirements/.
[16] Center on Budget and Policy Priorities, "Coordinating Medicaid and SNAP Work Requirements to Streamline Determinations," https://www.cbpp.org/research/health/coordinating-medicaid-and-snap-work-requirements-to-streamline-determinations.
[17] Code for America, "Work Requirements Implementation Toolkit," https://codeforamerica.org/resources/work-requirements-implementation-toolkit/.

Recommendation 6: Permit federal modernization funding to support interoperable evidence exchange

CMS should clarify that Government Efficiency Grants and applicable federal matching funds[18] may support open, interoperable capabilities for issuing, receiving, validating, and managing digital evidence used in eligibility determinations. Eligible expenditures could include issuer trust registries, credential validation services, beneficiary presentation tools, caseworker interfaces, credential status services, accessibility testing, and integration with existing eligibility systems.

Funding conditions should require conformance with published standards, portability across vendors, appropriate privacy and security controls, preservation of nondigital pathways, and transparent performance reporting. CMS should evaluate these investments using operational and beneficiary-centered measures, including ex parte verification rates, processing time, administrative cost, successful resolution of documentation requests, appeals, and procedural denial rates.

Recommendation 7: Establish voluntary state pilots before the 2028 documentation transition

CMS should invite interested states to pilot optional credential-based evidence submission during 2027. Each pilot should preserve all existing verification pathways, define authorized credential issuers and accepted data elements, establish accessibility and privacy safeguards, and interoperate with existing federal and state services rather than creating a separate eligibility system.[19] [20] CMS should also require an evaluation plan that measures processing time, successful verification, eligibility-worker effort, appeals, procedural denials, and beneficiary experience.

Pilot findings should be published in sufficient detail to inform national guidance before the post-2027 documentation requirements take effect. Neither coverage nor participation in any public benefit program should be conditioned on enrollment in a pilot or possession of a digital identity or credential.

Recommendation 8: Apply proportionate identity assurance without mandating a particular technology

When an individual elects to submit evidence digitally, CMS should require identity and authentication controls proportionate to the risk of the transaction and consistent with the CMS Interoperability

---

[18] Centers for Medicare & Medicaid Services, “CMS Launches Nationwide Framework to Implement Medicaid Work Requirements,” https://www.cms.gov/newsroom/press-releases/cms-launches-nationwide-framework-implement-medicaid-work-requirements.
[19] Centers for Medicare & Medicaid Services, “Eligibility Made Easy,” https://www.cms.gov/medicaid-chip/community-engagement-support/eligibility-made-easy.
[20] Center on Budget and Policy Priorities, “Understanding CMS’s EMMY Medicaid Work Requirement Tools,” https://www.cbpp.org/blog/understanding-cmss-emmy-medicaid-work-requirement-tools.

Framework[21] and NIST SP 800-63-4.[22] States should be permitted to accept multiple equivalent approaches, including appropriately assured state accounts and mobile driver's licenses, rather than requiring a single identity provider, application, or biometric method.

Identity proofing should not become a new barrier to Medicaid eligibility. States should preserve assisted and nondigital alternatives[23] for individuals who lack conventional identity documents, smartphones, reliable connectivity, or the ability to complete remote identity proofing.[24] Biometric verification should not be required as the sole means of access. Where printable or offline evidence is supported, CMS should establish clear validation and status-checking requirements before such evidence is used in an adverse eligibility decision.

III. Existing standards provide a foundation for implementation

CMS does not need to create a proprietary credential format to implement these recommendations. Existing standards provide mature building blocks for digitally signed credentials, holder-mediated presentation, mobile identity documents, and identity assurance. Relevant standards include the W3C Verifiable Credentials Data Model,[25] the ISO/IEC 18013 series,[26] OpenID for Verifiable Presentations,[27] and NIST SP 800-63-4.[28]

Technical standards alone are not sufficient. CMS and participating states would also need to define the program-specific trust framework, including authorized issuer categories, accepted claims, credential validity periods, revocation and status checking, evidence retention, audit procedures, accessibility

---

[21] Centers for Medicare & Medicaid Services, "CMS Interoperability Framework," https://www.cms.gov/health-technology-ecosystem/interoperability-framework.
[22] National Institute of Standards and Technology, Digital Identity Guidelines, NIST Special Publication 800-63-4, https://pages.nist.gov/800-63-4/.
[23] U.S. Department of Agriculture, Food and Nutrition Service, "Online Application Policy Clarification," https://www.fns.usda.gov/snap/online-application-policy-clarification.
[24] Digital Government Hub, "Digital Doorways to Public Benefits: User Experiences with Digital Identity," https://digitalgovernmenthub.org/publications/digital-doorways-to-public-benefits-user-experiences-with-digital-identity.
[25] World Wide Web Consortium, Verifiable Credentials Data Model v2.0, W3C Recommendation, https://www.w3.org/TR/vc-data-model-2.0/.
[26] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 18013-5:2021, Personal Identification—ISO-Compliant Driving Licence—Part 5: Mobile Driving Licence (mDL) Application; and ISO/IEC 18013-7, Personal Identification—ISO-Compliant Driving Licence—Part 7: Mobile Driving Licence (mDL) Add-on Functions.
[27] OpenID Foundation, OpenID for Verifiable Presentations 1.0, https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.
[28] National Institute of Standards and Technology, Digital Identity Guidelines, NIST Special Publication 800-63-4, https://pages.nist.gov/800-63-4/.

requirements, privacy protections, and the treatment of disputed or unavailable credentials. These decisions can build on infrastructure already operating in state digital identity programs and on federal reference architecture work, but they should be tested through controlled pilots before broad adoption. An example of a state digital identity program which has emphasized strong individual rights is Utah's State Endorsed Digital Identity (SEDI) framework, which was signed into law as SB 275 (2026).[29] This work is largely aligned with the ACLU's Digital ID State Legislative Recommendations (2024).[30]

Further, California and Utah demonstrate that standards-based credentials can operate in state government environments,[31] [32] while the NIST NCCoE reference architecture[33] and CMS Interoperability Framework[34] provide relevant federal foundations. Applying these technical patterns to Medicaid eligibility verification would extend existing infrastructure to a new program context rather than require CMS to develop an entirely new technical model.

IV. Conclusion

The community engagement requirement will require states to verify employment, education, service, income, and exemption information for a large and diverse population. CMS should design the implementation framework around the principle that eligible individuals should not lose coverage solely because an authoritative record is unavailable through automated data matching or because they cannot navigate a documentation process.

Maximized ex parte verification and automatic application of supported exemptions should remain the primary approach, which can be augmented to a higher bar of security and convenience using new technologies such as verifiable digital credentials in conjunction with data privacy frameworks. For cases that cannot be resolved through existing data, CMS should allow states to accept additional forms of reliable evidence, including optional, standards-based verifiable digital credentials issued within a defined trust framework and available to present from the user's device. These pathways

[29] Utah State Legislature, "State-Endorsed Digital Identity Program Amendments," 1st Substitute S.B. 275, 2026 General Session (introduced Feb. 24, 2026), https://le.utah.gov/Session/2026/bills/introduced/SB0275S01.pdf
[30] American Civil Liberties Union, "ACLU Digital ID State Legislative Recommendations," October 10, 2024, https://www.aclu.org/publications/aclu-digital-id-state-legislative-recommendations.
[31] California Department of Motor Vehicles, "mDL Adoption Statistics," https://www.dmv.ca.gov/portal/mdl-adoption-statistics/.
[32] Utah Division of Technology Services, "Verifiable Digital Credentials," https://dts.utah.gov/what-we-are-doing/our-initiatives/verifiable-digital-credentials/.
[33] National Cybersecurity Center of Excellence, National Institute of Standards and Technology, "Digital Identities—Mobile Driver's License (mDL)," https://www.nccoe.nist.gov/projects/digital-identities-mdl.
[34] Centers for Medicare & Medicaid Services, "CMS Interoperability Framework," https://www.cms.gov/health-technology-ecosystem/interoperability-framework.

should preserve beneficiary choice, protect sensitive information, support multiple vendors and technologies, and operate alongside paper, telephone, in-person, and assisted processes.

SpruceID would welcome the opportunity to provide technical input to CMS or participating states as they evaluate these approaches. Thank you for considering these comments.

Respectfully submitted,

Wayne Chang
Founder and Chief Executive Officer
Spruce Systems, Inc. (dba SpruceID)