ConnectedHealthInitiative

September 14, 2026

The Honorable Dr. Mehmet Oz
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS-3485-NC
P.O. Box 8016
Baltimore, Maryland 21244-8016

RE: Comments of the Connected Health Initiative on the *Request for Information; Clinical Laboratory Improvement Amendments of 1988 (CLIA) Regulations* [CMS-3485-NC; RIN 0938-AW01]

Dear Administrator Oz:

The Connected Health Initiative (CHI), an initiative of the Association for Competitive Technology (ACT), appreciates the opportunity to respond to the request for information (RFI) issued by the Centers for Medicare & Medicaid Services (CMS) and the Centers for Disease Control and Prevention (CDC) on the regulations implementing the Clinical Laboratory Improvement Amendments of 1988 (CLIA).[1] Those regulations were implemented in 1992, and several of the questions the agencies now ask reach directly into the work of the digital health community, including how laboratories use software algorithms and artificial intelligence (AI) in the postanalytic process, how facilities that process and interpret data without examining specimens should be treated, whether competency may be assessed through remote observation, and how laboratories should approach cybersecurity. CHI offers the views and recommendations below on those questions, together with a short response to the immunohematology question in section D.3, which raises the same issue about software in a different specialty. The comments follow the structure of the RFI, and each heading identifies the section and, where applicable, the question numbers to which the discussion responds. We take no position on the remaining topics, which fall outside the expertise of our membership.

CHI's comments are organized as follows:

[1] Request for Information; Clinical Laboratory Improvement Amendments of 1988 (CLIA) Regulations, 91 Fed. Reg. 43,586 (July 16, 2026) (CMS-3485-NC; RIN 0938-AW01).

I. Executive Summary

CHI is the leading multistakeholder policy and legal advocacy effort dedicated to connected health technologies that improve health outcomes and reduce costs. Our members build the software that laboratories, pathologists, and ordering clinicians increasingly rely on, and our recommendations on this RFI are summarized here.

- **Software and AI in the postanalytic process (Section B.6).** The software our members supply assists a qualified person rather than replacing one, and the result leaves the laboratory under the responsibility of the laboratory director or another authorized individual. CHI recommends that CMS and CDC preserve that structure, and that they distinguish software functioning as a component of a test system from software performing a discrete analysis that produces a separately reportable interpretation, because the two raise different questions.
- **Verification of software performance (Section B.6).** Laboratories already establish or verify performance specifications and maintain ongoing quality assessment, and software fits within that framework without new requirements. CHI recommends that the agencies address version control and revalidation on change through guidance, align that guidance with the Food and Drug Administration (FDA) framework for predetermined change control so laboratories are not held to two inconsistent standards, with a proportionate change control process for software that is not an FDA-authorized device, and reference recognized professional and imaging standards rather than writing technical specifications into the regulations.
- **Incorporating AI, automation, and cloud analytics into the regulations (Section B.6, question 5).** CHI recommends that the agencies proceed through interpretive guidance rather than new technology-specific regulatory requirements. Where a change to the regulations proves necessary, it should be written around what the software does to a result and what review that result receives, so that the requirement does not depend on a label that will describe different technology in five years.
- **Data-only facilities (Section B.7).** These entities perform work of several different kinds, and a single answer will not fit all of them. CHI recommends that the agencies draw the line at who issues the report, so that a vendor returning computational output to the reporting laboratory needs no certificate of its own while an entity issuing its own patient-specific report is already addressed by the existing definition, and that they confirm that transmitting data for computation is not distributive testing. No new certificate category built around software is needed, and accountability should continue to rest with the laboratory that selects the tool, verifies its performance, and reports the result.

- **Consistency with the CY 2027 payment rules (Section B.7).** CMS proposed in the CY 2027 physician fee schedule and hospital outpatient rules to reclassify algorithmic analyses of previously generated laboratory data partly on the reasoning that they do not require a CLIA-certified laboratory, while this RFI asks the same question from the other direction. CHI recommends that CMS answer it once, and that the answer turn on the nature of the service and on who stands behind the result rather than on where a computation physically occurs, and that CMS not finalize the CY 2027 laboratory analysis proposals until it has answered the question it poses here.
- **Remote direct observation (Section B.8).** CHI supports allowing remote observation for the direct observation element of competency assessment, as the Clinical Laboratory Improvement Advisory Committee recommended, described in terms of what the observer must be able to see and hear rather than by naming particular devices.
- **Cybersecurity (Section C.3).** CHI recommends that any expectation be risk-based and aligned with the frameworks laboratories already follow, that the agencies describe outcomes rather than mechanisms such as port and address restrictions, that they not adopt a location-based prohibition on access by personnel outside the United States, and that guidance confirm that cloud-hosted systems are consistent with CLIA obligations, since for many smaller laboratories a managed service provides stronger security than anything they could build themselves.

Each of these positions is developed in the sections that follow.

II. Introduction and Statement of Interest

CHI is the leading multistakeholder policy and legal advocacy effort dedicated to improving health outcomes while reducing costs through digital health innovation. CHI aims to realize an environment in which Americans see improvements in their health through policies that allow connected health technologies to advance outcomes and reduce costs. Our members develop and deploy connected health technologies across a wide range of use cases, including telehealth platforms, remote physiologic and remote therapeutic monitoring, software as a medical device, prescription digital therapeutics, clinical decision support, and AI-enabled diagnostic and workflow tools. We advocate before Congress, numerous federal agencies, and state legislatures and agencies on coverage and payment, privacy and security, health data interoperability, FDA regulation of digital health, and the role of AI in care delivery. For more information, see https://connectedhi.com.

CHI has developed, with the participation of clinicians, developers, health systems, and patient organizations, a set of publicly available resources on the responsible development and use of health AI, including our Policy Principles for Artificial Intelligence in Health, our Good Machine Learning Practices, and our Health AI Roles and Interdependency Framework, which allocates responsibility for safety and efficacy across the AI value chain.[2] CHI is also an appointed member of the American Medical Association's Digital Medicine Payment Advisory Group. These resources were built for exactly the question the agencies confront here, which is how to assign responsibility

[2] Connected Health Initiative, Policy Principles for Artificial Intelligence in Health, https://connectedhi.com/wp-content/uploads/2022/02/Policy-Principles-for-AI.pdf. CHI's Health AI Roles and Interdependency Framework and Good Machine Learning Practices white paper are also available at https://connectedhi.com.

among the laboratory, the clinician, the developer, and the organizations that deploy these tools, and CMS and CDC are welcome to draw on them directly.

Our interest in this RFI is practical. Laboratory medicine is where a great deal of clinical AI is actually being used today, and our members report that the principal obstacle is not the absence of rules but uncertainty about how the rules that already exist apply. Resolving that uncertainty would do more for patients than adding requirements, and CHI offers these comments in that spirit.

III. Software Algorithms and AI in the Postanalytic Process (Section B.6)

CMS explains that it has received multiple inquiries about which postanalytic activities it considers part of the testing process, and that test systems are becoming more complex and more integrated with advanced technology and AI systems. CHI appreciates the agencies' willingness to take the question up directly, because the uncertainty CMS describes is real and our members encounter it whenever they bring software into a laboratory workflow.

a. How Software Participates in Postanalytic Interpretation Today (Questions 1–3)

Taking the first three questions in section B.6 together, the software our members supply operates in the postanalytic phase as an aid to a qualified person rather than as a substitute for one. In next generation sequencing, software annotates and prioritizes variants, applies classification criteria drawn from published professional guidelines, and assembles the evidence on which a laboratory director or a certified molecular professional bases a final classification. In histocompatibility testing, software supports antibody assignment, epitope analysis, and virtual crossmatch calculations. In pharmacogenomics, software translates genotype into predicted phenotype and drafts interpretive language keyed to published dosing guidance. In histopathology, image analysis quantifies staining, identifies and counts objects such as mitotic figures, and directs the pathologist's attention to regions of a whole slide image, while the pathologist retains responsibility for the diagnosis. In each of these settings the result leaves the laboratory under the responsibility of the laboratory director or another individual authorized to report it, and CHI recommends that CMS and CDC preserve that structure, which places accountability with the person and the entity best positioned to exercise it.

CHI asks the agencies to keep two situations distinct, because they are easily conflated and they raise different questions. Software may operate as a component of a test system, performing a computation that has always been part of producing the result the laboratory reports, as when an analyzer's embedded algorithm converts a signal into a reportable value or a sequencing pipeline calls variants from raw reads. Software may instead perform a discrete analysis on data the laboratory has already produced and generate an interpretation that stands on its own as a separately reportable finding. The first is already governed by the requirements that attach to the test system as a whole, while the second raises the questions the agencies ask about data-only facilities, which CHI addresses in section IV.

The same analysis answers the question the agencies ask in section D.3 about electronic crossmatching. An electronic crossmatch is performed by a computer applying rules to previously determined blood type and antibody screen results in place of a serologic mixing step, with a qualified technologist reviewing the comparison and releasing the unit, so the software operates as a component of the test system rather than as a separate service and the laboratory remains

accountable for the result exactly as it is for a serologic method. CHI recommends that the agencies address electronic crossmatching through the same principle they apply to software elsewhere in the postanalytic process, under which the laboratory validates and monitors the system as it is actually used and the regulations do not attempt to specify the design of the algorithm.

b. Verification of Software Performance Under the Existing Framework (Question 4)

Question 4 asks what methods laboratories use to verify the performance of software functions, including image resolution and quality and the performance of computers and monitors. Laboratories do this today within the framework CLIA already provides, under which a laboratory must establish or verify performance specifications before reporting patient results and must maintain ongoing quality assessment thereafter.[3] Our members support laboratories in meeting those obligations by supplying intended use statements, validation summaries, known limitations, representative data sets, and advance notice of changes that could affect performance, and the laboratories then verify performance in their own hands, on their own specimen mix and instrumentation, before putting a tool into clinical use. CHI recommends the following clarifications, which would resolve most of what our members hear from laboratory customers:

- **Treat software as part of the test system it serves.** A laboratory verifying a test system that includes a software component should verify the system as it will actually be used, rather than validating the software separately against a standard that does not exist. Guidance confirming this would settle a recurring question without changing any laboratory's obligations.
- **Distinguish software that is fixed between releases from software that changes.** A model whose parameters are fixed behaves consistently and can be verified once and monitored thereafter, while a model that is updated or that adapts in use requires a defined change control process and revalidation when it changes. CHI recommends that the agencies state that expectation in guidance and align it with FDA's predetermined change control plan framework for device software, so that a laboratory using an FDA-authorized tool is not asked to satisfy two inconsistent standards for the same update. Because a predetermined change control plan is a device construct that a laboratory will not have for a rule engine in its information system or for software it configures itself, the guidance should call for a proportionate laboratory change control process in those cases, covering the version in use, the events that trigger revalidation, and notification when a supplier changes the software.
- **Reference recognized standards for imaging and display rather than writing specifications into the regulations.** Professional guidance on validating whole slide imaging for diagnostic use, together with established imaging and display standards, already addresses monitor calibration, resolution, color reproduction, and image quality, and those documents are revised as the technology changes. Numerical specifications written into the CLIA regulations would be out of date well before the next rulemaking cycle.
- **Keep documentation proportionate.** Much of the verification burden falls on small laboratories that have no dedicated informatics staff. CHI recommends that guidance describe what the laboratory must be able to show rather than prescribe a documentation

[3] 42 C.F.R. § 493.1253; see also 42 C.F.R. pt. 493, subpt. K.

format, and that it recognize supplier-provided validation materials as a legitimate part of the record.

The same reasoning answers the question in section B.4 about methods that may present performance characteristics the existing requirement does not address. For next generation sequencing, our members' experience is that accuracy, precision, analytical sensitivity and specificity, and reportable range can all be established for a bioinformatics pipeline, provided the agencies confirm that the pipeline as configured and used is part of the test system the laboratory verifies. What would not work is a requirement that the agencies review or approve pipeline design, which would place CMS and CDC in a role FDA already occupies for regulated software and would give laboratories no additional assurance about the results they report.

c. Whether Additional Technology Considerations Belong in the CLIA Regulations (Question 5)

Question 5 asks whether additional technology considerations, including automation, cloud analytics, and AI, should be incorporated into the CLIA regulations for high complexity testing. CHI's view is that the agencies can accomplish what they need through interpretive guidance, and that adding technology-specific requirements to the regulations would create obligations overlapping with those that laboratories and developers already carry under CLIA itself, under FDA's device framework, and under the security and privacy rules that govern health information, and CHI recommends the following:

- **Begin with guidance.** Updating the interpretive guidelines in Appendix C of the State Operations Manual, issuing a memorandum to surveyors and accrediting organizations, and training the survey workforce, informed by the Clinical Laboratory Improvement Advisory Committee, would let the agencies address automation, cloud analytics, and software-assisted interpretation at the pace the technology actually moves, and would let them correct course without a rulemaking.
- **Write any requirement around function rather than around a technology label.** A requirement that names AI will be both overinclusive and underinclusive, because a long-standing rule engine in a laboratory information system may fall within the label while a consequential new analytic method falls outside it. Framing any expectation around what the software contributes to the reported result, and what human review that result receives, produces a requirement that holds as the underlying methods change. The same concern applies to the question in section D.1 about recognizing additional specialties, and CHI recommends that if the agencies do so they not treat software-assisted interpretation as a specialty or certificate category of its own, which would divide a laboratory's work according to the tools it uses rather than the testing it performs.
- **Avoid duplicating FDA oversight.** Where a software function is a regulated device, FDA already reviews its design, evidence, and postmarket obligations. CLIA is well suited to address how a laboratory selects, verifies, monitors, and uses a tool, and CHI recommends that the agencies keep to that ground rather than assessing the design of the tool itself.
- **Confirm that cloud-based analysis is compatible with CLIA.** Our members and their laboratory customers would benefit from a plain statement that a laboratory may use cloud infrastructure and remotely executed analysis while meeting its obligations for record retention, availability, confidentiality, and control of the testing process, and that the infrastructure provider does not thereby become a laboratory. Many smaller laboratories

depend on these services for capabilities they could not otherwise offer, and the absence of a clear statement has caused some to hesitate. In doing so the agencies should state the operational expectations a surveyor will apply, which are that the laboratory remains responsible for the availability and retrieval of its records for the retention periods the regulations set, including where a vendor relationship ends, and that a business associate agreement addresses privacy and security without displacing that obligation.[4]

- **Match any new expectation to survey capacity.** Requirements that would ask surveyors to evaluate algorithm design or model performance would be difficult to apply consistently across the survey workforce, and inconsistent application is itself a burden on laboratories and developers. CHI recommends that the agencies consider what can be assessed reliably in a survey before settling on what to require.

IV. Data-Only Facilities (Section B.7)

The agencies ask what activities data-only facilities perform to generate, or help to generate, test results and interpretations, and they frame the question against the definition of a laboratory as a facility for the examination of materials derived from the human body for the purpose of providing information for the diagnosis, prevention, or treatment of disease or the assessment of health.[5] This is the most consequential question in the RFI for CHI's membership, because the answer determines whether entities that never receive a specimen are drawn into a certification regime built around facilities that do.

a. What Data-Only Facilities Do (Question 1)

Drawing on our members' experience, the entities that might be described as data-only perform work of several different kinds, and CHI recommends that the agencies keep them separate rather than treating them as a single category:

- **Computational processing returned to the ordering laboratory.** Secondary and tertiary analysis of sequencing data, including alignment, variant calling, and annotation, performed on data the laboratory generated and returned to that laboratory, which reviews the output and reports the result under its own certificate.
- **Image analysis on laboratory-generated images.** Quantification, object detection, and triage performed on whole slide images or other images the laboratory produced, again returned to the laboratory and to the pathologist who signs the report.
- **Derived values and risk scores.** Calculations performed on results a laboratory has already reported, sometimes combined with clinical information, producing a score or a probability rather than a new measurement of a biological material.
- **Independent interpretation services.** An entity applies clinical or scientific expertise to data produced elsewhere and issues its own patient-specific interpretation, which reaches the ordering clinician as that entity's report, and many of these entities hold CLIA certificates today.
- **Infrastructure and platform services.** Storage, computation, transmission, and hosting of laboratory information systems, involving no clinical judgment about any patient's result.

[4] 42 C.F.R. § 493.1105.

[5] 42 C.F.R. § 493.2.

These differ in what they contribute to the reported result and, more importantly, in who stands behind that result, so a single answer about whether a data-only facility requires certification will not fit all of them.

b. Certification Should Continue to Follow the Reporting Laboratory

The existing definition turns on the examination of materials derived from the human body. An entity that performs such an examination and issues its own patient-specific result or interpretation is doing what the definition describes, and the existing framework applies to it without amendment, which is why many independent interpretation services hold certificates today. The definition does not by its terms reach a vendor that receives data, returns computational output to a certified laboratory, and leaves that laboratory to review the output and report the result under its own certificate. In that arrangement the laboratory is the entity the definition reaches, and it is the laboratory that chooses the tool, verifies its performance in its own setting, decides how the output is used, and answers for the result.

The definition of distributive testing the agencies quote points the same way, describing testing performed on the same specimen, or an aliquot of it, that must be shared between two or more laboratories to obtain the data needed for a final reportable result.[6] Sending data for computation and receiving the output back for the ordering laboratory to review and report involves no sharing of a specimen or an aliquot and is therefore not distributive testing, while sending data to an entity that issues its own report to the ordering clinician raises the question the agencies appear to have in mind. CHI recommends that the agencies say so plainly, because laboratories and their suppliers are presently left to guess at it. CHI recommends that the agencies draw the line in those terms and take the following steps:

- **Draw the line at who issues the report, and create no certificate category for developers, vendors, or infrastructure providers.** An entity that returns computational output to the reporting laboratory should need no certificate of its own, while an entity that issues its own patient-specific report to the ordering clinician is already addressed by the existing definition, and neither case calls for a new certificate type built around software. Extending certification to entities that never receive a specimen and never issue a result would duplicate obligations these companies already carry under FDA's device framework and under the privacy and security rules, would add nothing to the accountability the reporting laboratory already bears, and would fall hardest on the small developers who supply a large share of the innovation in this area and who cannot absorb a second certification regime. The likely practical effect would be fewer suppliers rather than safer testing.
- **Clarify what a laboratory should obtain from its suppliers.** Guidance describing the intended use statement, validation summary, statement of limitations, change notification commitment, and support arrangements a laboratory should secure, and confirming that obtaining and reviewing them discharges the laboratory's obligation with respect to a purchased component, would give both sides a workable standard. CHI's Health AI Roles and Interdependency Framework sets out this allocation of responsibility across the value chain in detail and is available to the agencies for that purpose.

[6] 42 C.F.R. § 493.2 (defining "distributive testing").

- **Address the referral question directly.** Where a laboratory sends data to another entity that returns an interpretation, guidance should say whether the arrangement is treated as a referral, whose report reaches the ordering clinician, and how the reporting and recordkeeping obligations are divided. Our members report that this, rather than any question about AI, is the practical ambiguity laboratories raise most often.
- **Phase any change and preserve access.** A substantial share of genomic, histocompatibility, and digital pathology testing depends on arrangements of this kind today. If the agencies conclude that some category of entity should be certified, CHI urges a clearly defined scope, a realistic transition period, and an assessment of the effect on patient access before any requirement takes effect.

c. Reconciling This Inquiry With the CY 2027 Software as a Medical Service Proposals

CHI raised a closely related question with CMS in comments filed on August 31, 2026, in the CY 2027 physician fee schedule docket.[7] There CMS proposed to move 10 codes describing algorithmic analyses performed on previously generated laboratory data off the Clinical Laboratory Fee Schedule and to price them under the physician fee schedule, reasoning in part that the analyses are entirely computer-based and do not require a CLIA-certified laboratory, with a companion proposal in the hospital outpatient rule.[8] CHI urged CMS to look at what the service is rather than at where a computer could in principle run it, and to preserve existing treatment where an analysis remains embedded in a CLIA-certified laboratory's testing process.

The same question now comes to the agency from the other direction, since this RFI asks whether facilities that perform only data processing and interpretation should hold certification at all. CHI recommends that CMS answer the question once and apply the answer consistently, so that whether a computational analysis belongs to a laboratory service turns on the nature of the service and on who validates and stands behind the result rather than on the physical location of the computation. If the agencies conclude under CLIA that such an analysis remains part of the laboratory's testing process, the premise of the payment proposal deserves reexamination, and if they conclude otherwise, they should say so plainly so that laboratories, developers, and Medicare contractors can plan against a settled understanding. In practical terms, CHI recommends that CMS not finalize the CY 2027 laboratory analysis proposals until it has answered the question it poses in section B.7, and that both instruments apply the same test, which is who validates the analysis and who signs the result. What our members cannot work with is one answer in the payment rules and a different one under CLIA.

V. Remote Direct Observation for Competency Assessment (Section B.8, Questions 1–3)

CHI supports allowing remote technology to be used for the direct observation element of competency assessment, as the Clinical Laboratory Improvement Advisory Committee

[7] Comments of the Connected Health Initiative on the CY 2027 Medicare Physician Fee Schedule and Quality Payment Program Proposed Rule (Aug. 31, 2026), https://connectedhi.com/wp-content/uploads/2026/09/CHI-Comments-on-CY-2027-Medicare-PFS-and-QPP-Proposed-Rule-31-Aug-2026-2.pdf.

[8] Comments of the Connected Health Initiative on the CY 2027 Hospital Outpatient Prospective Payment and Ambulatory Surgical Center Payment Systems Proposed Rule (Aug. 31, 2026), https://connectedhi.com/wp-content/uploads/2026/09/CHI-Comments-re-CMS-Draft-2027-OPPS-Rule-31-Aug-2026-1.pdf.

recommended at its November 2024 meeting and as the agencies describe in the RFI. The current provisions require direct observation of routine patient test performance and of instrument maintenance and function checks as part of the technical consultant's or technical supervisor's evaluation, and nothing in that purpose requires the observer to be physically present when the observation can be conducted reliably through video.[9] Our members supply many of the video, collaboration, and workflow tools that laboratories would use for this purpose, and we offer the following recommendations:

- **Permit remote observation at the discretion of the technical consultant or technical supervisor.** The person responsible for the assessment is best placed to judge whether a particular element can be observed adequately at a distance, and the regulation should allow that judgment rather than mandating one mode.
- **Describe what the observer must be able to see and hear rather than naming devices.** The RFI asks which devices laboratories use, and the honest answer is that the mix changes constantly and that smartphones, tablets, headsets, and fixed video systems each suit different tasks. A requirement expressed in terms of an unobstructed view of the specimen, the instrument, and the operator's actions, adequate audio for questions in both directions, and confirmation of the identity of the person being observed will still make sense when the devices have changed.
- **Do not require recording.** Recording introduces privacy, security, and retention obligations without improving the assessment, and laboratories should be free to conduct the observation live. Where a laboratory chooses to record, existing safeguards for protected health information apply.
- **Recognize the benefit to rural, small, and multi-site laboratories.** As the advisory committee observed, facilities in rural areas stand to gain the most, and the same is true of laboratories with off-shift staff and of health systems whose technical supervisors cover several sites. Travel cost and scheduling are real obstacles to timely competency assessment, and removing them supports both compliance and staffing.
- **Allow a hybrid approach.** A laboratory should be able to conduct some competency elements remotely while retaining on-site observation where the task or the individual warrants it, without having to justify the mix element by element.

VI. Cybersecurity (Section C.3, Questions 1–4)

CHI agrees with the agencies' description of the threat environment. Laboratories depend on laboratory information systems, electronic health record integration, automated instrumentation, and remote access, and an incident affecting any of these interrupts patient care as surely as an instrument failure. Our members build those connected systems and carry security obligations of their own, both contractually and as business associates. Our recommendations concern how the agencies should express any expectation rather than whether security deserves attention:

- **Align with the frameworks laboratories already follow rather than creating CLIA-specific requirements.** A laboratory that is a covered entity or a business associate is already subject to the HIPAA Security Rule, and Congress has directed the Department to consider an entity's adoption of recognized security practices, including the Health Industry Cybersecurity Practices developed under section 405(d) of the Cybersecurity Act

[9] 42 C.F.R. §§ 493.1413(b)(8), 493.1451(b)(8).

of 2015 and the NIST Cybersecurity Framework.[10] CHI recommends that the agencies recognize conformity with a recognized framework as satisfying any CLIA expectation, which would improve security practice while adding no new compliance architecture.

- **Describe outcomes rather than mechanisms.** The RFI asks how laboratory systems restrict ports and internet protocol addresses, which describes one implementation of network control. Cloud-hosted and modern on-premises systems increasingly rely on identity-based access, segmentation, and continuous verification rather than fixed addresses, and a requirement written around ports and address ranges would push laboratories toward older architectures that are not more secure. CHI recommends that any expectation be stated as an outcome, which is that access is limited to authorized users and systems and is logged and monitored, with the mechanism left to the laboratory and its vendors.
- **Do not adopt a location-based restriction on access.** The RFI asks whether individuals or entities outside the United States are ever allowed to access systems containing personal information. CHI recommends against a prohibition framed around location, because where a person sits is a weak proxy for risk compared with how they are authenticated, what they are authorized to reach, whether the session is encrypted and logged, and what their employer is contractually bound to do. Existing federal requirements already occupy this ground, including the business associate framework and the Department of Justice rule restricting access to bulk sensitive personal data by countries of concern, and a separate CLIA restriction would add compliance work without adding protection. A flat restriction would also disrupt the follow-the-sun support and security monitoring that many laboratories, particularly smaller ones, rely on for coverage outside business hours, which would leave them less well protected rather than more.
- **Confirm that cloud-hosted systems are consistent with CLIA obligations.** For most small and mid-sized laboratories, a managed cloud service delivers patching, monitoring, backup, and incident response at a standard they could not reach on their own. Guidance should make clear that using such services is compatible with the laboratory's obligations for records, availability, and confidentiality, so that security expectations do not inadvertently discourage the arrangement that most improves security.
- **Align incident response and reporting with existing channels.** Laboratories and their vendors already report incidents through breach notification requirements and, for covered entities, through federal cyber incident reporting. CHI recommends that the agencies rely on those channels rather than establishing a separate CLIA reporting obligation, since duplicate reporting consumes the staff who are needed on the response itself during the hours that matter most.
- **Assign responsibility without creating a position.** The RFI asks which laboratory job position is responsible for cybersecurity. In most laboratories that function sits with an enterprise security team or with a managed service provider rather than with laboratory personnel, and that is generally the better arrangement. CHI recommends that guidance require responsibility to be assigned and documented rather than vested in a named laboratory role, which in a small laboratory would amount to an unfunded position filled by someone without the relevant training.

[10] See Pub. L. No. 116-321 (2021) (directing the Department to consider a covered entity's or business associate's adoption of recognized security practices); Health Industry Cybersecurity Practices, developed under section 405(d) of the Cybersecurity Act of 2015; and the NIST Cybersecurity Framework 2.0.

- **Keep training proportionate and practical.** Security awareness training is already a widespread practice and a HIPAA requirement, and CHI recommends that the agencies point laboratories to existing resources, including the materials developed under section 405(d), rather than specifying curriculum or frequency in the regulations.

VII. Conclusion

CHI appreciates the agencies' willingness to examine how a regulatory framework built in 1992 applies to the way laboratory medicine is practiced today. The questions on software-assisted interpretation, data-only facilities, remote competency assessment, and cybersecurity are the right ones to be asking, and in each case CHI believes the agencies can resolve the uncertainty our members encounter through interpretive guidance that explains how the existing requirements apply, rather than through new technology-specific obligations that would duplicate what laboratories and developers already carry. The one question that will not resolve itself is the treatment of computational analysis performed on previously generated laboratory data, where CMS has taken one view in its CY 2027 payment rules and is asking an open question here, and CHI urges the agency to settle that point consistently across both workstreams.

We look forward to working further with CMS, CDC, and other stakeholders on these questions, and we would welcome the opportunity to discuss any of these recommendations in greater detail.

Sincerely,

Brian Scarpelli
Executive Director

Chapin Gregor
Policy Counsel

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005
p: +1 517-507-1446
e: bscarpelli@healthismobile.org