Notice of Funding Opportunity for Rural Health Cybersecurity Grant Program

Rural Health Transformation Program Activity 6.4
NOFO No. 2027-Cyber-01

Massachusetts Technology Collaborative
75 North Drive
Westborough, MA 01581-3340
http://www.masstech.org

Procurement Team Leader:	**Maxwell Fathy**
NOFO Issued:	**November 10, 2026**
Answers to Questions Posted:	**December 2, 2026**
Responses Due:	**Rolling**

1. INTRODUCTION

1.1 Overview

Massachusetts Technology Collaborative ("MassTech"), on behalf of the MassCyberCenter is issuing this Notice of Funding Opportunity (NOFO No. 2027-Cyber-01) for the Rural Health Cybersecurity Grant Program to solicit responses from rural health facilities ("RHFs") interested in receiving grants ("Applicants'") to fund cybersecurity services, which include assessments, Managed Detection and Response ("MDR"), and other related managed cybersecurity services. The submissions of all Applicants shall be evaluated pursuant to the evaluation criteria set forth in this NOFO.

MassTech will act as the contracting entity on behalf of the MassCyberCenter and (except where the specific context warrants otherwise) MassCyberCenter and MassTech are collectively referred to as MassTech, and any singular reference to MassTech or MassCyberCenter shall mean and apply to both entities interchangeably throughout this NOFO. MassTech will enter into an **RHTP Cybersecurity Subrecipient Grant Agreement** (the "Agreement") with selected Applicants. This Agreement is the form of contract MassTech expects to use for awards under this NOFO, and its terms include federal requirements that are mandatory conditions of award. Selected Applicants who execute this Agreement with MassTech will receive federal pass-through funding and will be considered federal subrecipients as defined in 2 CFR § 200.1. NOFO Attachment B, the Code of Federal Regulations and Centers for Medicare & Medicaid Services RHTP Flow-Down Requirements for Subrecipients, sets out additional federal requirements that apply to funded organizations and must be passed on to any lower tier subrecipients. Attachment B is incorporated into the Agreement. Applicants should review all NOFO attachments as well as the posted Agreement template before applying. Submitting an application confirms that the Applicant is able and willing to comply with required terms and has reviewed all documents. Please note that these documents may be updated to comply with changes in MassTech, EOHHS or federal requirements.

This NOFO is funded by the Centers for Medicare & Medicaid Services ("CMS") of the U.S. Department of Health and Human Services ("HHS") as part of a financial assistance award totaling $162,005,238.13 with 100 percent funded by CMS/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by CMS/HHS, or the U.S. Government.

1.2 MassTech and the MassCyberCenter

MassTech is an independent public instrumentality of the Commonwealth of Massachusetts chartered by the Commonwealth to serve as a catalyst for growing its innovation economy. MassTech brings together leaders from industry, academia, and government to advance technology-focused solutions that lead to economic growth, job creation, and public benefits in Massachusetts. For additional information about MassTech and its programs and initiatives, please visit our website at www.masstech.org.

The MassCyberCenter has a vision for a diverse, vibrant, and competitive Massachusetts cybersecurity ecosystem that enhances resiliency for public and private entities, provides workforce development opportunities, and elevates public cybersecurity awareness. The Center carries out this vision through its mission to convene the Massachusetts cybersecurity ecosystem to improve cybersecurity resiliency, workforce development, and public awareness within the state by developing cutting edge programs, organizing engaging events, and leading collaborative working groups. For more information about MassCyberCenter and its programs and activities generally, please visit the website at https://masscybercenter.org.

2. Grant Overview

2.1 Background

In 2025, the Rural Health Transformation Program ("RHTP") was authorized pursuant to Section 71401 of Public Law 119-21 (One Big Beautiful Bill Act). This federal initiative provides funding to states to support rural communities in improving health care access, quality, and outcomes by transforming the health care delivery ecosystem. The Centers for Medicare and Medicaid released a notice of funding opportunity for all states for a total of $50 billion over five budget periods to support the goals of RHTP. The NOFO directed states to propose uses of the funding to meet RHTP's strategic goals, including fostering the use of innovative technologies to help transform the way care is delivered in rural communities. The Commonwealth of Massachusetts included in their proposal a program to administer cybersecurity implementation grants to financially constrained rural providers, enabling them to adopt security technologies and best practices.

Massachusetts will receive approximately $162 million in federal funding for federal fiscal year 2026 as part of this new five-year initiative and a portion of this funding will support the launch of the Rural Health Cybersecurity Grant Program. This program provides RHFs in Massachusetts with grants to fund cybersecurity services from CyberTrust Massachusetts.

2.2 CyberTrust Massachusetts Overview

CyberTrust Massachusetts is a non-profit organization working closely with the MassCyberCenter and is currently supported with grant funding to provide governance to Security Operations Center ("SOC") and Cyber Range facilities located at colleges and universities across the Commonwealth to grow the cybersecurity talent pipeline, as well as help provide solutions to municipalities, small businesses, and other organizations for protection against cyber threats. SOC services are provided to customers as part of a paid subscription.

CyberTrust Massachusetts is also employing students from its academic members to help provide these SOC services under the supervision of industry experts while receiving workforce training and development opportunities that will prepare them to enter cybersecurity careers.

CyberTrust Massachusetts was formed in 2022 through a grant from the Massachusetts Cybersecurity Innovation Fund, which is administered by the MassCyberCenter. For more information about CyberTrust Massachusetts, visit https://www.cybertrustmass.org/.

2.3 *Services Eligible for Grant Funding*

RHFs in Massachusetts are eligible to receive grants to fund cybersecurity services, including assessments, Managed Detection and Response, and other managed related services, from CyberTrust Massachusetts. Grants are eligible to fund the following CyberTrust Massachusetts services, including, but not limited to:

Cybersecurity Assessments

- Evaluation against standard industry cybersecurity frameworks with criteria specific to healthcare delivery environments
- Technical testing of key aspects of defenses

Virtual CISO ("vCISO") and Training

- Cybersecurity Strategy & Roadmap: Develop a practical, prioritized improvement plan based on patient safety, organizational risk, HIPAA requirements, available resources, and operational needs
- Continuous compliance management: Monitoring, policy upkeep, evidence collection, and control validation
- Proactive gap detection: Early identification and remediation of control drift, config issues, and documentation gaps

- Hands-on consulting to help implement security improvements, integrate new systems, strengthen security processes, and respond to significant security incidents
- Assist organizations with interpreting the HIPAA Security Rule and emerging federal healthcare cybersecurity requirements
- Cybersecurity training for RHF staff, to include cybersecurity awareness and professional upskilling

Managed Detection and Response ("MDR")

- Managed endpoint detection and response using a SentinelOne technology stack: 24/7 monitoring of endpoints, threat insights, proactive notifications, consultations on handling threats and false positives, and threat response
- Active threat hunting, based on cyber threat intelligence, malicious actor tactics, and known bad resources, identifies new and unique threats
- Software inventory including vendor, version, footprint
- Asset discovery using active and passive scanning across the network
- Operating system and third-party vulnerability analysis and enrichment

Extended Detection and Response ("XDR") — broader monitoring across key systems

- Extends existing SentinelOne EDR with cross-source detection across identity, email, and firewall — no new platform required
- Monitors a defined set of critical integrated log sources, including Active Directory, Entra ID, email security, and firewall; additional integrations available as needs grow
- Correlates activity across sources to detect additional threats, such as phishing-related compromise, account takeover, and lateral movement
- Automated detection and alerting, with analyst review and escalation to your team on high-confidence incidents
- Supports cyber insurance requirements, compliance reviews, and incident investigations through consolidated activity records across monitored systems

Application Control and Zero Trust

- Control over which applications can run on your systems, using the ThreatLocker technology stack
- Containment of unauthorized software and programs
- Reduced attack surface and lateral movement opportunities
- Can be applied broadly across all assets, or selectively across high-value assets and users

Email Security

- Advanced detection of phishing and email-based attacks
- Automatic removal of dangerous attachments and malicious links

These services will enable rural health providers to adopt modern cybersecurity procedures and tools establishing a culture of shared understanding around the need for all health data exchange to be private and secure.

Selected RHFs will be required to comply with quarterly and annual reports to support the completion of state reports for CMS under the RHTP program. Reporting templates and submission deadlines will be provided by the MassCyberCenter.

2.4 Funding Eligibility

RHFs in Massachusetts that meet the following definitions are eligible to apply for funding:

- Rural Hospital
- Rural Health Clinics
- Rural-Located or Rural-Serving Federally Qualified Health Center (FQHC)
- Rural Municipalities
- Rural-Located Community-Based Organization (CBO) / Social Service Organization (SSO)
- Rural-Located Healthcare Provider or Practice
- Rural-Located Nursing Facilities
- Emergency Medical Services (EMS) / Ambulance Provider

Definitions for each of these entities can be found in the Rural Health Transformation Program (RHTP) Rural Partners RFA located here.

Other categories of RHFs may be eligible, subject to approval of the Massachusetts Executive Office of Health and Human Services.

3. Grant Requirements and Guidance

Applicants must first receive a scope of work from CyberTrust Massachusetts for cybersecurity services for one year. Grants will fund up to the full cost of the scope of work for the year of services.

Selected Applicants will be eligible to receive grants to continue the services in subsequent years up to a total of 5 years subject to the continued availability of RHTP funding. Grants may fund the following amounts of the annual cost of the scope of work:

Year	Grant Percent of Scope of Work Cost*
1	Up to 100
2	Up to 100
3	Up to 100
4	Up to 67
5	Up to 33

**Funding percentage of scope of work may differ for Rural Municipalities compared to other categories of RHFs.*

Applicants must include the scope of work as part of their application. To develop a scope of work, RHFs should contact rhtpcyber@masstech.org.

4. Evaluation Process and Criteria

To receive funding as set forth within this NOFO, an Applicant must:

- meet the funding eligibility requirements per section 2.4; and provide a scope of work for cybersecurity services from CyberTrust Massachusetts.
- Projects that include both assessments and managed services from CyberTrust Massachusetts will be prioritized.

MassTech shall evaluate each application that is properly submitted. As part of the selection process, MassTech may invite Applicants to answer questions regarding their application. In its sole discretion, MassTech may also choose to enter into a negotiation period with an Applicant and then ask the Applicant to submit additional information.

Lack of debarment status by either the state or federal government is also required.

The goal of this NOFO is to select and enter into a grant agreement with the Applicant that will most closely align with MassTech Collaborative's goals in the publication of this NOFO. MassTech reserves the right to consider such other relevant factors as it deems appropriate.

5 APPLICATION PROCESS

5.1 Application and Submission Instructions

Applicants are cautioned to read this NOFO carefully and to conform to its requirements. Failure to comply with the requirements of this NOFO may serve as grounds for rejection of an Application**.**

a. All applications must be submitted HERE.
b. Applications shall include:
    i. A brief overview of the Applicant, including: a description of the RHF**,** location of operations, and number of employees**.**
    ii. Scope of Work for Cybersecurity Services:
        - The scope of work from CyberTrust Massachusetts for services.
        - A non-confidential description of how services will assist the respondent in developing a mature cybersecurity program (250 words maximum).
    iii. Authorized Applicant's Signature and Acceptance Form (Attachment A**)**, which contains specified certifications by Applicant. Please read the certifications carefully before signing.
    iv. A copy of the respondent's W-9

Any responses, applications, data, materials, information and documentation submitted to MassTech in response to this NOFO shall become MassTech's property and be subject to public disclosure. As a public entity, the MassTech is subject to the Massachusetts Public Records Law (set forth at Massachusetts General Laws Chapter 66). There are very limited and narrow exceptions to disclosure under the Public Records Law. If an Applicant wishes to have the MassTech treat certain information or documentation as confidential, MassTech the Applicant shall clearly label only the information and/or documentation they believe is confidential or proprietary as "**CONFIDENTIAL**" in the application. MassTech's receipt of such documents does not represent a finding by MassTech's or the Supervisor of Public Records that such documents are exempt from public disclosure, and they may be disclosed if an applicable exemption does not apply.

5.2 Application Timeframe

MassTech will review applications on a rolling basis. Awards will be issued until all program funds are expended.

Grants may only fund expenses incurred after an application is submitted to MassTech. *Note: submission of an application is not a guarantee of receiving an award from MassTech*, *and Applicants must assume all project costs if the application is not selected for an award.*

5.3 Questions

Questions regarding this NOFO must be submitted by electronic mail to rhtpcyber@masstech.org with the following Subject Line: "Questions – NOFO No. 2027-Cyber-01**."** MassTech will post responses to questions received on the MassTech website beginning on December 2, 2026. Responses to all questions received will also be posted to the Comm-Buys website.

6.0 GENERAL CONDITIONS

6.1 General Information

a. If an application fails to meet any material terms, conditions, requirements or procedures, it may be deemed unresponsive and disqualified. MassTech reserves the right to waive omissions or irregularities that it determines to be non-material.
b. This NOFO, as may be amended from time to time by MassTech, does not commit MassTech to select any firm(s), pay any costs incurred in preparing an application or in connection with the award of any contracts. MassTech reserves the right, in its sole discretion, to make no awards through this NOFO, to withdraw the NOFO, to engage in preliminary discussions with prospective applicants, to accept or reject any or all applications received, to request supplemental or clarifying information, to negotiate with any or all qualified applicants, and to request modifications to applications in accordance with negotiations, all to the same extent as if this were a Request for Information.
c. Unless otherwise specified in this NOFO, all communications, responses, and documentation must be in English, and all cost applications or figures in U.S. currency. All applications must be submitted in accordance with the specific terms of this NOFO.
d. On matters related to this NOFO that arise prior to an award decision by MassTech, applicants shall limit communications with the MassTech to the NOFO Team Leader and such other individuals as the MassTech may designate from time to time. No other MassTech employee or representative is authorized to provide any information or respond to any questions or inquiries concerning this NOFO. Applicants may contact the NOFO Team Leader for this NOFO if it is incomplete.
e. MassTech may provide reasonable accommodations, including the provision of materials in an alternative format, for applicants with disabilities or other hardships. Applicants requiring accommodation shall submit requests in writing, with supporting documentation justifying the accommodation, to the NOFO Team Leader. MassTech reserves the right to grant or reject any request for accommodation.
f. Applicant's submissions shall be treated by MassTech as an accurate statement of applicant's capabilities and experience. Should any statement asserted by applicant prove to be inaccurate or inconsistent with the foregoing, such inaccuracy or inconsistency shall constitute sufficient cause for MassTech in its sole discretion to reject the application and/or terminate of any resulting agreement.

6.2 Posting of Modifications/Addenda to NOFO

This NOFO has been distributed electronically using MassTech, MassCyberCenter and COMMBUYS websites. If MassTech determines that it is necessary to revise any part of this NOFO, or if additional data is necessary to clarify any of its provisions, an addendum will be posted to the websites. It is the responsibility of each potential Applicant to check MassTech, MassCyberCenter and COMMBUYS websites for any addenda or modifications to the NOFO. MassTech accepts no liability and will provide no accommodation to applicants who submit a response based on an out-of-date NOFO.

Attachment A
Authorized Applicant's Signature and Acceptance Form

The undersigned is a duly authorized representative of the Applicant listed below. The Applicant has read and understands the NOFO requirements. The Applicant acknowledges that all of the terms and conditions of the NOFO are mandatory. By executing this Authorized Applicant's Signature and Acceptance Form, Applicant certifies that they (1) are in compliance with the terms, conditions and specifications contained in this NOFO, (2) acknowledges and understands the procedures for handling materials submitted to MassTech as set forth in the NOFO, (3) agrees to be bound by those procedures, and (4) agrees that MassTech shall not be liable under any circumstances for the disclosure of any materials submitted to MassTech pursuant to this NOFO or upon the Applicant's selection.

The Applicant understands that, if selected by MassTech, the Applicant and MassTech will execute an agreement specifying the mutual requirements of participation. The Applicant agrees that the entire bid response will remain valid for sixty (60) days from receipt by MassTech.

Applicant: _____

(Printed Name of Applicant)

I certify that Applicant is in compliance with all corporate filing requirements and State tax laws. I further certify that the statements made in this response to the NOFO, including all attachments and exhibits, are true and correct to the best of my knowledge.

By: _____

(Signature of Authorized Representative)

Name: _____

(Signatory's Printed Name)

Title: _____

Date: _____

Applicant's UEI No.: _____

Attachment B

Code of Federal Regulations and Centers for Medicare & Medicaid Services RHTP Flow-Down Requirements for Subrecipients

PART 1: FEDERAL SUBAWARD IDENTIFICATION DATA

Element	Information
Subrecipient name and UEI	[Subrecipient name and UEI - TBD]
Federal Award Identification Number (FAIN)	RHTCMS332069
Federal award date	December 29, 2025
Assistance Listing number and title	93.798, Rural Health Transformation Program
Federal awarding agency	Centers for Medicare & Medicaid Services (CMS), HHS
Pass-through entities	EOHHS; Mass Tech Collaborative
Awarding Entity	Massachusetts Technology Collaborative (*or, if* Subrecipient *is completing a new Part 1 for a lower-tier subaward in accordance with Section 1.3(c) below,* Subrecipient *as the Awarding Entity*)
Total federal award	$162,005,238.13
Total MassTech master obligation	$49,993,125.00
Track 2.4 Program Track Ceiling	$14,120,000.00 (Rural Digital Health Sandbox Program) -Years 1-3 not-to-exceed
Track 2.5 Program Track Ceiling	$12,287,500.00 (Rural SHINE-HT Program) - Years 1-3 not-to-exceed
Track 6.1 Program Track Ceiling	$13,860,000.00 (Rural Health Information Exchange) -Years 1-3 not-to-exceed
Track 6.4 Program Track Ceiling	$9,725,625.00 (Rural Health Cybersecurity) - Years 1-3 not-to-exceed
Applicable RHTP program track for this Subaward	[TBD - completed at award]
Subaward amount	[Completed at award based on active project budget]
Subaward period of performance	[Completed at award]
Awarding Entity contact	[Grantor Project Manager identified in Exhibit 1, Section 2 - name, title, email, phone]

PART 2: STANDARD FEDERAL COMPLIANCE TERMS AND FLOWDOWN REQUIREMENTS

1. Applicability, Funding Source, and Compliance/Flow-Down Obligations

1.1 **Applicability.** The compliance requirements outlined in this Attachment B will be incorporated into and made a part of any final Agreement between MassTech (the "Awarding Entity") and selected Applicants (the "Subrecipient(s)," as defined in 2 CFR § 200.1). Upon execution of an Agreement, Subrecipient shall be fully responsible for all compliance covenants outlined in this Attachment.

1.2 **Funding Source.** This Subaward is funded in whole or in part by the Centers for Medicare and Medicaid Services (CMS) of the U.S. Department of Health and Human Services (HHS), under the Rural Health Transformation Program (RHTP). These federal pass-through funds are administered by

MassTech via the Commonwealth of Massachusetts Executive Office of Health and Human Services (EOHHS).

- **Federal Awarding Agency:** Centers for Medicare and Medicaid Services (CMS) / HHS
- **Federal Program:** Rural Health Transformation Program (RHTP)
- **Total Master Federal Award:** $162,005,238.13 (100% federally funded)
- **MassTech Maximum Obligation:** $49,993,125.00

1.3 **Federal Lobbying Compliance, Flow-Down, and Execution Obligations.**

(a) Federal Lobbying Compliance. All awarded Applicants shall execute a Certification Regarding Lobbying as part of their Agreement with MassTech,. This certification language must be included in all Subrecipient lower-tier subawards, subgrants, and subcontracts exceeding $100,000.

(b) Post-award: Downstream Execution and Reporting. After award and contracting with MassTech, Subrecipients shall flow down and incorporate Part 2 of this Attachment B (excluding instructions) into every lower-tier agreement or subaward funded in whole or in part with these funds. **For each downstream award, Subrecipients shall independently**:

1. Complete a new Part 1 data block detailing that specific lower-tier subrecipient's financial allocations;
2. Obtain an authorized signature from the lower-tier subrecipient on a *Lower-Tier Subrecipient Acknowledgment* block to legally bind them to these terms;
3. Require the lower-tier subrecipient to execute a separate copy of Certification Regarding Lobbying prior to disbursing any funds, if the downstream project budget exceeds $100,000; and
4. Deliver copies of all executed downstream acknowledgments and certifications to MassTech within thirty (30) days of execution for federal audit review.

2. Compliance

2.1 Federal award terms. Subrecipient shall comply with all applicable federal award terms and conditions, including applicable RHTP requirements, as they apply to the Subaward. Subrecipient shall ensure that all expenditures and activities funded under the Subaward, including those of its subcontractors and subrecipients, are allowable, reasonable and necessary under the Subaward, the RHTP Notice of Funding Opportunity, the Notice of Award, and all other applicable state and federal requirements.

2.2 Compliance with laws. Subrecipient shall comply with all applicable statutes, orders and regulations of any federal, state, municipal or other governmental authority relating to its property or its operations under the Subaward.

2.3 Debarment and exclusion. Subrecipient represents that no owner, employee, consultant or subcontractor of Subrecipient has been debarred by any federal agency, excluded from participation in a program under Titles XVIII, XIX or XXI of the Social Security Act, or subjected to a civil money penalty under the Social Security Act.

2.4 Lower tier agreements. Subrecipient shall incorporate all applicable federal award terms and conditions, including applicable RHTP requirements, into any subcontract or lower tier subaward funded in whole or in part with Subaward funds. Subrecipient shall ensure that each subcontractor or lower-tier subrecipient it intends to use is permissible under the Subaward and shall identify and report each one to the Awarding Entity before executing an agreement with it. Subrecipient acknowledges that MassTech's agreement with EOHHS may require EOHHS's prior approval of subcontractors and lower-tier subrecipients, and Subrecipient shall not execute an agreement with any such entity until the Awarding Entity confirms approval in writing. Subrecipient shall maintain sufficient oversight of all such subcontractors and lower-tier

subrecipients and ensure that each complies with this Attachment B, all other applicable requirements of the Agreement, and all federal and state laws.

2.5 Scope changes. Subrecipient shall not make material changes to the scope of work or activities undertaken under the Subaward without the prior written approval of the Awarding Entity.

2.6 Use of funds. Subrecipient shall use Subaward funds only for the activities and budget approved in the Subaward, consistent with the uses of funds permitted under Section 71401 of Public Law 119-21 and the RHTP Notice of Funding Opportunity (CMS-RHT-26-001). Unless otherwise permitted by CMS and approved in the Subaward, Subrecipient shall not use Subaward funds for:

(a) costs incurred before the start of the Subaward period of performance;

(b) matching or cost-sharing requirements of any other federal award or of any local entity;

(c) services, equipment or supports that another party is legally required to provide under federal, state or tribal law, including civil rights law, such as required workplace modifications or accommodations;

(d) goods or services that are not allocable to the project;

(e) replacing existing state, local, tribal or private funding for infrastructure or services, including staff salaries;

(f) new construction, building expansion, purchase of buildings, major retrofits, cosmetic upgrades, or other costs that substantially increase the value or extend the useful life of an asset, except minor renovations and alterations that are clearly tied to program goals, approved in the Subaward, and approved in advance by CMS;

(g) independent research and development, including its share of indirect costs;

(h) lobbying or any activity intended to influence legislation, appropriations, regulations, administrative actions or executive orders, as prohibited by 2 CFR 200.450 and the HHS Grants Policy Statement;

(i) covered telecommunications or video surveillance equipment or services under 2 CFR 200.216, or household subsidies for broadband installation or monthly internet service;

(j) meals, except for study subjects and patients, meals specifically approved as part of the project, or meals within a per diem or subsistence allowance for allowable travel;

(k) clinical services reimbursable by insurance, services that duplicate billable services, or changes to existing fee schedule amounts;

(l) specified sex-trait modification procedures, as defined at 45 CFR 156.400;

(m) clinician salaries or wage support, except as part of an RHTP initiative approved by CMS, and in no case at any facility that imposes non-compete restrictions on its clinicians;

(n) any expenditure related to intergovernmental transfers, certified public expenditures, or other financing of a non-federal share; or

(o) any payment not permitted under Section 2105(c)(1), (7) or (9) of the Social Security Act, including the limitation on payment for abortions and the citizenship documentation requirements for payments for individuals.

3. Reporting

3.1 Project reports. Subrecipient shall submit, at least quarterly, progress reports, as well as interim and final reports, using the templates and deadlines the Awarding Entity provides, and shall ensure that any subcontractors or lower-tier subrecipients complete such reporting on their progress under their subcontracts or subawards. Reports shall include reporting on key performance indicators and shall align with any other reporting requirements from CMS or EOHHS.

3.2 Expenditure reports. Subrecipient shall submit quarterly and annual reports on expenditures and activities in alignment with the reporting requirements from CMS or EOHHS and shall ensure that any subcontractors or lower-tier subrecipients complete such reporting for their expenditures and activities.

3.3 Program metrics. Subrecipient shall provide the data the Awarding Entity needs to report on the program metrics and key performance indicators for the applicable RHTP program.

4. Records, Audit, and Data Security

4.1 Records. Subrecipient shall maintain all books, records and other compilations of data pertaining to the Subaward, to the extent and in such detail as properly substantiate claims for payment, in a cost effective and easily retrievable format for a minimum period of six (6) years from the date the final expenditure report is submitted to the Commonwealth or until all pending federal or state audit findings are fully resolved, whichever occurs later.

4.2 Audit compliance and framework. The Subrecipient shall comply with all applicable federal subrecipient audit requirements, including the Single Audit framework under 2 CFR Part 200 Subpart F (historically referred to, and tracked by the Commonwealth as, OMB Circular A-133). Subrecipient shall provide MassTech with a copy of its annual Single Audit report, or an official threshold exemption certification, within nine (9) months of the end of the Subrecipient's fiscal year.

4.3 Audit and inspection. The Awarding Entity, MassTech, EOHHS, the Governor, the Secretary of Administration and Finance, the Comptroller, the State Auditor, the Attorney General, any of their authorized representatives or designees, and any other state or federal oversight agency shall have the right, at reasonable times and on reasonable notice, to:

(a) Examine and copy books, records and other compilations of data pertaining to the Subaward;

(b) Evaluate the quality, appropriateness and timeliness of Subrecipient's performance;

(c) Inspect and audit Subrecipient's financial records related to the Subaward; and

(d) Audit, inspect, and view the Subrecipient's active real-time financial tracking dashboard, ledger systems, and live cost tracking setups.

4.4 Real-Time Recording and Ledger Access. The terms and conditions of the federal award require that expenses be recorded in real-time. Subrecipient shall record all costs chronologically in its financial systems at or near the time the liability was incurred. In addition, to support oversight by the Awarding Entity, MassTech, EOHHS, and federal auditors, the Subrecipient shall make its active financial dashboard or ledger immediately available upon request and must demonstrate that all costs claimed for reimbursement were so recorded, in a format that permits continuous reconciliation against the specific categorical caps and line items defined in the project budget.

4.5 Safeguards. Subrecipient shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of personal information and any other data and materials used under the Subaward.

4.6 Documentation. Subrecipient shall maintain, and readily produce to the Awarding Entity upon request, sufficient documentation to support, demonstrate, and justify that each expenditure under the Subaward is allowable, reasonable and necessary, and shall ensure that all subcontractors and lower-tier subrecipients maintain, and produce to Subrecipient upon request, such documentation for their expenditures. Such documentation may be requested for any lawful purpose, including a state or federal audit.

5. Public Communications

5.1 Prior approval. Subrecipient shall obtain prior approval from the Awarding Entity and, where the Awarding Entity is not MassTech, from MassTech, before Subrecipient or any of its officers, agents or employees responds to any media inquiry, makes any public comment or issues any other public communication, or authorizes the issuance, display, distribution or publication of any news story, publicity release, interview, promotional or marketing material, or other public announcement regarding any aspect of the Subaward. Subrecipient shall also ensure that its subcontractors or lower-tier subrecipients obtain prior approval from Subrecipient before issuing any such public statements. Subrecipient acknowledges that MassTech may be required to obtain approval from EOHHS before approving any such communication.

5.2 Federal funding disclosure. Where Subrecipient identifies the source of Subaward funding in approved materials, it shall state that the work is "supported by the Centers for Medicare & Medicaid Services (CMS) of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling **$162,005,238.13** with 100 percent funded by CMS/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by CMS/HHS, or the U.S. Government."

6. Recovery of Funds and Termination

6.1 Recovery of funds. To the extent payments are made under the Subaward for purposes later determined to be impermissible under the Subaward, the Massachusetts RHTP grant, or other state or federal law by EOHHS, CMS, a federal or state auditor, or another oversight agency, the Awarding Entity may recoup or recover those funds from Subrecipient.

6.2 Termination for loss of funding. The Awarding Entity may terminate the Subaward on cessation in whole or in part of state or federal funding for the program, or on changes in applicable state or federal law or initiatives that make termination necessary or advisable.

6.3 Amendment for compliance. The Awarding Entity may amend the Subaward as necessary to comply with federal RHTP requirements, or to implement and comply with state or federal statutory or regulatory requirements, judicial orders, settlement agreements, or any state or federal initiatives or changes affecting the Awarding Entity, the Subrecipient or the Subaward.