

As part of the technical plan described in Section 5.2.2, applicants should include responses to the following tasks. Applicants should only address the questions and components of questions most relevant to the project scope. Not all questions apply to the scope of work in each grant category.

1. Provide a key point of contact to coordinate any follow up or questions on the technical plan that the HEAL NY Phase 5 Health IT project team may have regarding your response.
2. Provide an executive summary for the technical plan containing an overview of all major points detailed in the technical plan and an explanation of how the proposed solution's strategy addresses the key principles described herein, including the common HIE protocol, core HIE services and suite of standards, interoperable EHRs, use cases (Attachment 7.1) and technical discussion document (Attachment 7.2).
3. Provide vendor(s) and health care software product(s) names included in your proposed solution including version, current release, new products in development and a description of how each product or component fits into the overall proposed solution.
4. Provide and describe a technical architecture and deployment model including major design principles, elements and integration strategy
5. How does EHR technical architecture enable integration of 3<sup>rd</sup> party software? Describe any current 3rd party connectivity/integration with your EHR (e.g., formulary and prescribing services, practice management systems, decision support providers, results delivery, including labs, pharmacy and provider reports, CPOE, Scheduling systems)
6. Prioritize essential components of the core HIE services, e.g., privacy and consent; reconciling patient IDs across RHIOs, etc., and discuss which, if any, aspects could be centralized across regions versus those that are distributed regionally.
7. Describe the technology used to develop and deploy your solution and how it will demonstrate the use case (s).
8. Describe or storyboard how your solution will meet the workflows considered as part of the use cases and how each component of your proposed solution is utilized throughout the workflow. Also, please describe the differences in workflow between the multi-regional vs. regional processes and community processes, if applicable.
9. List and describe data standards that your proposed solution supports at each phase of the workflow. Standards are required to be consistent with current and emerging federal standards, as recognized by the Secretary of HHS.
10. How would the implementation of the SHIN-NY common HIE protocol, core services and suite of standards align with, build upon and inform the NHIN trial implementation pilots?
11. Describe your strategy for historical data loading including services offered and recommendations.

12. Describe how your solution is able to respond to new clinical systems and technologies from an interoperability and integration perspective.
13. Define how your solution interfaces to existing source systems and list any standard formats proposed. Include how information can be captured as well as disseminated from your solution.
14. Describe your ability and timeline to demonstrate your proposed solution as a pilot implementation.
15. Describe your application's approach with regards to intellectual property and source code management.
16. Describe how the solution would be deployable to additional physician practices and organizations within and across communities or regions in a scaleable manner and the incremental technical, financial and operational implications associated with expansion at both data provider and administrative components. Please describe the ongoing support and maintenance that will be necessary for your solution.
17. What privacy and security considerations, including patient consent and compliance with relevant rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are implicated by your solution, and how could they be addressed?
18. Describe how your proposed solution addresses the privacy and security considerations described in Section 5.2.1.11 and 5.2.2.12.
19. Please describe the system performance for the proposed solutions. In addition to the items below, list any requirements and other factors that could influence performance of the system:
  - a. Response time for a transaction (average, maximum)
  - b. Capacity (for example, the number of concurrent customers or transactions the system can accommodate)
  - c. Average system response time after user input
19. Please describe system safeguards that prevent users from severely degrading system performance or "hanging" the system (e.g. searches that return a large number of records).
20. Address the following questions regarding system availability, backup and recovery:
  - a. What is the backup, recovery and archival plan for data and system availability? Describe your infrastructure to support it.
  - b. Describe your application's availability requirements in terms of redundancy or fault tolerance. What are the implementation requirements for maximum system availability?
  - c. Does the application allow for a limited mode of operation (e.g. continued operation in event of a disaster)?
  - d. Describe the aspects of the system which allow continued usability when certain services or entities are not available (offline) during planned maintenance windows, unplanned outages, or become unavailable during events when primary service providers are not able to provide power, internet service, or land and cell communications.

21. Please provide the contact information for 3 current references for the health information service provider partners. The references may be contacted by the HEAL NY team without prior notice.
22. Describe any future plans for strategic partnerships that involve health care software products for health information service provider partners.
23. Do you have a designated and independent information security officer and security plan? Does the plan include formal processes for risk assessment, code review, intrusion detection, vulnerability scanning, enterprise antivirus software implementation, and event response? Does your security officer oversee your identity management and access control (e.g., firewall) infrastructure? Does your security officer participate in design, development and implementation of all external facing services?
24. Please describe how your proposed solution will provide capabilities for secure data delivery, confirmation of delivery, data integrity and non-repudiation checking, and audit logging error handling for data access.