After reviewing all the questions received by Friday October 4th 2019, the most common and relevant questions were chosen and the answers are below. No additional question will be answered.

- Should facility walkthroughs for all 10 locations (main hospital, nursing home, plus 8 remote locations) be included in the RFP?
  Main Hospital (NUMC), Nursing Home (AHP), and 3 randomly chosen LIFQHC locations. All locations are within Nassau County, New York.

- Should we include in our proposal a data discovery effort so that the identification of other sources of ePHI can be documented?
  Yes.

- Does the scope include a security audit of a sample of the Business Associates?
  Assessor should examine security related certificates from 5 randomly chosen Business Associates.

- Does the scope include a review of training-related policies and procedures, and evaluation of a sample of Workforce Member knowledge?
  Yes.

- Network Architecture Designs review also include wireless networks?
  Yes.

- How many separate entities are there?
  2.
  NuHealth, includes Nassau University Medical Center and A. Holly Patterson Extended Care Facility.
  LIFQHC.

- Are there any network-enabled medical devices that store or transmit ePHI?
  Yes.

- How many data centers and where are they located?
  1 data center in Nassau County, New York.

- Are any of the applications hosted at cloud providers?
  No.

- When did NHCC perform their last Assessment?
  2018.

- What is the time frame for completing the Assessment?
  By the end of 2019.

- Will NHCC have a project manager assigned to the Assessment to facilitate interviews, document request and facility assessments?
  Yes

- Will reporting be separate for Nassau University Medical Center, A. Holly Patterson Extended Care Facility, and the LIFQHC locations?
  There should be 1 report for NuHealth (Nassau University Medical Center and A. Holly Patterson Extended Care Facility) and 1 report for LIFQHC.

- Does NUMC and AHP have the same HIPAA Security Rule policies and procedures?
  Yes.

- Does LIFQHC have the same HIPAA Security Rule policies and procedures?
  No.

- How many EHRs does NuHealth operate?
  Information will be provided during assessment.

- Who are NuHealth's EHR vendors?
  Information will be provided during assessment.

- Are the EHR(s) hosted or operated in house?
  Hosted.

- Would you like to include external and internal vulnerability scanning, penetration testing, or both as part assessment?
  Both.

- Have there been any recent acquisitions or other organizational changes that have significantly impacted the IT/IS function?
  No.

- Is the intent of the assessment to be a HIPAA Security Gap Assessment, where awarded firm is auditing the implemented HIPAA Program as compared to the HIPAA Security Rule or is the intent of the assessment to conduct your annual HIPAA Security Risk Analysis which provides both a gap assessment of the rules and the holistic risk assessment needed to fulfil 164.308(a)(1)(ii)(A)?
  The purpose of this assessment is to comply with HIPAA and MU/PI Security Risk Analysis which provides both a gap assessment of the rules and the holistic risk assessment needed to fulfil 164.308(a)(1)(ii)(A).

- You are requesting us to list all projects for the past (18) months. Again, all of our "current" and "past" projects are subject to Non-Disclosure Agreements (NDA) and confidentiality agreements

that are in place and specific information cannot be furnished at this time. Are we able to provide limited (generic) information regarding the current projects in its place?
Yes, customer name or identifiable information can be redacted, or replace with generic information to satisfy your NDA or confidentiality agreements.

- Can a list of systems be provided either in detail or in summary?
  Information will be provided during the assessment.

- Will the hospital sign an NDA that permits large privately held proposers to release their financial statements? Can this be done in time to meet the aggressive response deadline?
  Please provide as much information as you can in the proposal.

- As a large firm, we have led thousands of projects over the last 18 months. We assume it's OK to list only those in our Risk and Compliance Practice; please provide guidance.
  Listing only those in our Risk and Compliance Practice is acceptable.

- Does corporate IT managed the infrastructure, hardware, and software at all locations?
  Yes.

- Does the quantity of workstations outlined in the RFP include mobile/portable/handheld devices?
  Yes.

- Does Nassau want the scope of the risk assessment to include medical devices that process, transmit, store or access ePHI?
  Yes.

- Will previous risk assessments be provided to the assessor?
  No.

- Can all locations (logically) be reached from one network location?
  Yes.

- Is the system accessible from the Internet?
  Only through VPN or Secure Remote Desktop.

- Is the system(s) accessible by a Third Party?
  Yes.

- Does the system(s) transmit or receive data with a third party/business partner?
  Yes.

- Are Mobile devices used in the environment?
  Yes.

- Based on the affiliation with Northwell Health, are any of its (Northwell) facilities within scope?
  No.

- Who is paying Expenses/Travel?
  The services should be provided on a fixed fee basis including all Expenses/Travel.

- Is the HIPAA Risk Assessment applicable to the security rule as well as the privacy rule and breach notification rule for this project?
  Only the security rule.

- Is there a current IT security policy manual?
  We have written Corporate Policies and Procedures that address our IT security.