The Grady Memorial Hospital Corporation
d/b/a

GRADY HEALTH SYSTEM

Remarkable Service Exceptional Care

GRADY HEALTH SYSTEM

Procurement & Strategic Sourcing

REQUEST FOR INFORMATION
(RFI)

FOR
Electronic Security and Access Control System
RFI# 26009TD

Request for Information Posted: 11/05/2026
RFI Responses Due: 11/20/2026
RFI assessment Completed by: 12/05/2026
RFI due: 12/30/2026

Questions regarding this solicitation are to be submitted to:
Toccara Denham
tmolyneaux@gmh.edu

GRADY HEALTH SYSTEM BACKGROUND

Grady Health System ("GHS") is one of the Southeast's largest public hospital systems. With a delivery system that includes affiliations with public health organizations, medical education programs, and community advocates, GHS provides quality, cost-effective, and customer focused health care to residents of metropolitan Atlanta and citizens of the State of Georgia. Grady Health System is comprised of Grady Memorial Hospital (953 licensed beds), Crestview Health and Rehabilitation Center (388 licensed long-term care beds), the Infectious Disease Center (HIV/AIDS), the Loughlin Radiation Oncology Center, the Maloof Imaging Center, six (6) community health centers, the Regional Perinatal Center, the State of Georgia Poison Control Center, the Georgia Cancer Center for Excellence, The Marcus Stroke and Neuroscience Center, Grady EMS-Atlanta's 911 ambulance service, the region's premiere Level I trauma center and nationally renowned emergency medicine and burn centers.

Grady Memorial Hospital opened in 1892 to provide medical care for indigent and emergency health care for all residents of the Atlanta community. Grady is currently operated by the Grady Memorial Hospital Corporation d/b/a Grady Health System. Medical care is provided under contract with Emory University and Morehouse Schools of Medicine. GHS also operates three (3) professional training programs in medical technology, radiation oncology, and radiation technology. GHS averages more than 25,000 inpatient visits and more than 600,000 outpatients annually, including over 95,000 emergency care visits (including psychiatric emergencies).

Request for Information (RFI)

The purpose of this RFI is to obtain information necessary to establish the technical approach, scope, budget, implementation strategy, and procurement requirements for replacement of the existing system. This RFI is for information and planning purposes and does not constitute a commitment by the Grady to purchase equipment or award a contract.

The existing system has reached operational limitations, and Grady is evaluating replacement options. The replacement system shall provide a modern, dependable, secure, scalable, and maintainable access control platform while minimizing disruption to facility operations. Grady currently operates an electronic access control system consisting of equipment, software, field devices, network infrastructure, locking hardware, credentials, and integrations from different generations and manufacturers.

Project Overview

Grady is seeking information from qualified electronic security and access control system providers for the design, supply, installation, integration, testing, commissioning, training, documentation, warranty, and ongoing support of a comprehensive electronic access control system (EACS) to replace the current system. The new EACS must be scalable to sufficiently support the access control platform and enable the design and production of chip-enabled employee ID badges.

Qualifications & Features

The primary objectives are to:

- Replace obsolete or unsupported access control equipment.
- Improve system reliability and availability.
- Improve cybersecurity and system resiliency; while addressing encryption, secure authentication, multi-factor authentication, role-based access, password policies, privileged access, audit logging, firmware security, software patching, vulnerability management, secure remote access, network segmentation, certificate management, security monitoring, backup security.
- Maintain or improve existing access control functionality.
- Provide a modern administrative interface.
- Provide migration strategy and maintain existing security operations during migration.
- Minimize replacement of functional field equipment where technically and economically appropriate.
- Provide a scalable platform for future expansion.
- Integrate with existing security and enterprise systems.
- Improve reporting, auditing, alarm management, and system monitoring.
- Provide a practical migration path from the existing platform to the replacement system.
- Establish a sustainable lifecycle and support model in terms of system resiliency.

State the expected behavior when:

A. The access control server is unavailable.
B. The network connection is unavailable.
C. A controller fails.
D. Power is interrupted.
E. Cloud connectivity is lost.

Provide following Qualifications:

- Company profile.
- Years in business.
- Relevant licenses.
- Manufacturer certifications.
- Security industry certifications.
- Number of qualified technicians.
- Number of system programmers/engineers.
- Local service capability.
- Relevant replacement projects.
- References.

Provide References:

Client:
Facility:
Location:
Project Size:
Existing System:
Replacement System:
Number of Doors:
Number of Users:
Project Value:
Completion Date:
Scope:
Reference Contact:
Phone/Email:

Request for Information (RFI)

Specifications / Description:

The anticipated project includes, but is not necessarily limited to:

- Full Assessment and documentation of the existing access control system.
- Design of a replacement access control system and proposed network architecture diagram
- Furnishing of new access control hardware and software.
- Replacement or reuse of existing field devices where appropriate and identify anticipated risks.
- Replacement of access control panels/controllers.
- Integration with existing door hardware and security systems where feasible.
- Migration of existing users, credentials, access levels, and schedules.
- Integration with the Grady's IT/network environment.
- Integration with video surveillance, intrusion detection, fire alarm, elevator, parking, and other systems as applicable.
- Removal and disposal of obsolete equipment.
- Describe Installation and programming methodology.
- Provide a comprehensive testing and commissioning plan.
- Staff training.
- As-built documentation.
- Warranty and ongoing maintenance/support.

The respondent shall provide a proposed methodology for developing a complete existing system inventory and identify any equipment for which compatibility with the proposed replacement platform has not been verified.

The inventory should include:

Equipment	***Manufacturer***	***Model***	***Serial No.***	***Quantity***	***Location***	***Condition***	***Reuse/Replace***
Controller							
Reader							
Lock							

Door Position Switch	
REX	
Power Supply	
Server	
Workstation	

Respondents must describe any proposed replacement access control platform by addressing:

- Web-based administration.
- System architecture.
- User administration.
- Credential administration.
- Access-level management.
- Scheduling.
- Holiday schedules.
- Temporary access.
- Visitor access.
- Alarm management.
- Reporting.
- Audit trails.
- Mobile administration.
- Remote administration.
- System monitoring.
- Automated workflows.

Respondents must also describe the process for migrating the existing system's:

- Personnel records.
- Credential numbers.
- Credential status.
- Existing facility codes
- Existing card technology
- Access levels.
- Door groups & hardware
- Time schedules.
- Holiday schedules.
- Alarm configurations for emergency and life-safety systems
- Operator accounts.
- Audit/history data
- Security System integration should identify whether each integration is; native, API-based, middleware-based, third-party, or not available.
  As well as include:
  A. Video surveillance/VMS.
  B. Intrusion detection.
  C. Intercom.
  D. Visitor management.
  E. Fire alarm.
  F. Elevator controls.

G. Parking access.
H. Vehicle gates.
I. Building management systems.
J. Emergency notification.
K. Security operations center systems

Identify any information that cannot be migrated and explain whether existing credentials can remain in service or whether new credentials will be required. If new credentials are required, describe the recommended credential technology and migration process.

Respondents are to provide documentation for the following:

- Existing-condition survey.
- Equipment inventory.
- Final system architecture.
- Network diagrams.
- Door schedules.
- Controller schedules.
- Device schedules.
- Wiring diagrams.
- Programming documentation.
- Database backup.
- Configuration backup.
- Software licenses.
- User manuals.
- Administrator manuals.
- Maintenance manuals.
- Test reports.
- Training materials.
- Warranty documentation.
- Recommended spare-parts list.

Provide standard response times for:

Priority	Example	Remote Response	On-Site Response
Critical	System-wide failure	[ ]	[ ]
High	Multiple doors unavailable	[ ]	[ ]
Medium	Individual door failure	[ ]	[ ]
Low	Non-critical issue	[ ]	[ ]

BUDGETARY PRICING

Provide budgetary pricing organized into:

Existing-System Assessment

- Site survey.
- Documentation.
- System assessment.

New System

- Controllers.
- Readers.
- Software.
- Servers.
- Licenses.
- Power supplies.
- Batteries.
- Network equipment.
- Other equipment.

Reuse

Identify cost savings associated with reuse of existing equipment.

Installation

- Removal.
- Installation.
- Wiring.
- Programming.
- Configuration.
- Integration.
- Testing.

Migration

- Database migration.
- Credential migration.
- Access-level migration.
- Phased cutover.

Training and Documentation

Recurring Costs

- Software licensing.
- Cloud subscription.
- Support.
- Maintenance.
- Mobile credentials.
- Other recurring fees.

Pricing shall clearly distinguish between **capital costs** and **recurring operating costs**.

RESPONDENT QUESTIONS

Respondents shall provide specific answers to the following:

1. What replacement platform do you recommend?
2. Why is this platform appropriate for replacement of the existing system?
3. What existing equipment can be reused?
4. What equipment must be replaced?
5. Can existing credentials be retained?
6. Can the existing access-control database be migrated?
7. What data cannot be migrated?
8. Can the existing VMS be integrated?
9. Can the existing fire alarm interface be retained?
10. Can existing locking hardware be retained?
11. What network changes are required?
12. What cybersecurity improvements will the new system provide?
13. Can the system operate during network/server outages?
14. What is the recommended migration sequence?
15. How will security be maintained during cutover?
16. What is the estimated implementation duration?
17. What areas will require service interruptions?
18. What are the major project risks?
19. What information is required fromGrady?
20. What equipment should Grady consider replacing even if it is technically reusable?
21. What equipment should be retained to reduce project cost?
22. What future technologies should be incorporated?
23. What recurring licensing costs will apply?
24. What is the expected useful life of the proposed platform?
25. What alternatives could reduce the total cost to Grady?

RESPONSE FORMAT

Responses shall be organized as follows:

1. Cover Letter.
2. Executive Summary.
3. Understanding of Existing-System Replacement Requirements.
4. Company Qualifications.
5. Relevant Experience.
6. Existing-System Assessment Methodology.
7. Recommended Replacement Strategy.
8. Proposed System Architecture.
9. Existing Equipment Reuse Analysis.
10. Hardware Replacement Requirements.
11. Software and Licensing.
12. Database/Credential Migration.
13. Integration Requirements.
14. Cybersecurity.
15. Phasing and Cutover.
16. Testing and Commissioning.
17. Training.
18. Documentation.
19. Maintenance and Support.
20. Warranty.
21. Lifecycle.
22. Schedule.
23. Risks and Mitigation.
24. Budgetary Pricing.
25. Alternates.
26. Exceptions and Assumptions.
27. References.
28. Product Data.

APPENDIX C: SOLICITATION/CONTRACT FORM

REQUEST FOR INFORMATION NUMBER: RFI# 26009TD

RFI DESCRIPTION: Electronic Security and Access Control System

PROPOSAL RESPONSES MUST ARRIVE NO LATER THAN **11/020/2026**

NOTE: Mark the outside lower-left corner of your submission with the RFI number shown above.

This document contains 10 pages. Questions regarding RFI**# 26009TD** should be directed to Toccara Denham tmolyneaux@gmh.edu **no later than 11/13/2026.**

You are invited to submit your Proposal for the services listed within this RFI. Responses must arrive at:

Electronic Responses accepted:

Executive Director
Materials Management: _____ DATE: _____

PLEASE BE ADVISED: Offerors must **complete and return all pages** required with Proposal submission. Failure to return these completed pages with responses may result in non-consideration of Proposal submission.

Please acknowledge receipt of the following Addenda to the solicitation documents below by entering the number and the date of each:

Addendum No.: _____ Date: _____

Addendum No.: _____ Date: _____

NAME OF RESPONDING FIRM: _____

NAME OF COMPANY OFFICER: _____
(Company officer must have authority to legally bind the company)

TITLE: _____

DATE:

_____

(MANDATORY) SIGNATURE OF COMPANY OFFICER ABOVE (Certifying agreement with specifications, terms and conditions unless otherwise noted).

_____

Signature