Grady Health System

Policy Name: **Third Party Access and Vendor Adherence**	Policy Number: **IS-01-105 Rev003**
Department: **Information Services**	Approval Date: **02/7/2020**
Division: **Information Security**	Effective Date:
	Retired Date: **00/00/0000**

PURPOSE

Granting system access to a third party provider is a risk that can introduce security threats and technical business dangers to Grady Health System's (GHS) network and information systems. This document outlines the steps third party providers must follow, and identifies policies and requirements for access to GHS's information resources.

CHANGE SUMMARY

The following is a brief summary of the changes that have been made to this document:

- Removed reference to IS-04-104 as that policy is no longer active.
- Added Architecture Review requirements
- Reference to updated Joint Commission standards

Note that this is only a summary. It is your responsibility to read the complete document to ensure you abide by the required elements.

SCOPE

This policy applies to all GHS Workforce. The GHS Workforce includes, but is not limited to, employees, medical staff, interns, visitors, contractors, students, volunteers and Business Associates.

POLICY STATEMENT

Grady Health System (GHS) may permit a third party provider to create, receive, maintain, or transmit information on its behalf only if there is a written agreement establishing the following procedural elements between GHS and the third party provider that grant assurances that the provider will appropriately safeguard the information.

PROCEDURES

THIRD PARTY CONTRACTS

1) All third party information services and technology contracts must be reviewed and approved by a representative from the GHS Legal Department. In addition, approval must also be obtained from IT Security for services where access to the GHS data network is required.
2) For contracts involving systems with HIPAA implications (e.g. ePHI or EDI transactions), the HIPAA Security Officer or Compliance Officer must ensure that the systems are operating within the guidelines of VPN access as outlined by IT Security.

3) Vendors wishing to contract with GHS must be GHS approved and registered with Vendormate. The Vendormate program is responsible for obtaining background information of vendors with whom GHS wishes to contract. This background information may include financial statements or customer referrals.
4) The HIPAA Security Officer and IT Security will define the security requirements of the third party and potential actions to be taken for violations of these requirements. The GHS Legal Department will ensure these requirements are part of the contract and that the third party is bound contractually to uphold GHS's information security policies and procedures. These requirements should include the following, but are not limited to:
    a. Agreement on acceptable security controls and policies;
    b. Determination of acceptable service levels and availability;
    c. Documentation of physical and logical controls employed by the third party to protect the confidentiality, integrity, and availability of GHS's data and equipment;
    d. Agreement that the third party must test and maintain system security at its location on an ongoing basis;
    e. The right for GHS to audit the third party's physical and logical environment for security controls surrounding the company's data and systems;
    f. Determination of all legal requirements including privacy and data protection;
    g. Commitment that the third party will immediately inform GHS of any security breaches that it becomes aware, including unauthorized access to or compromise of company data or resources; and
    h. Determination of ownership of any software developed or intellectual property obtained by outside personnel (e.g., contractors) while servicing

ACCESS CONTROLS

1. Third party organizations are required to adhere to the same access restrictions as internal GHS users. These requirements are documented in the ***IS-01-103: Password Requirements and Management*** and ***IS-01-101: Computer Systems Acceptable Use*** policies.
2. Access to information will be granted by IT Security on a "need to know" basis and limited to related requirements.
3. Access requests will be closely monitored to detect possible security exposures to the GHS environment. All exceptions are at the discretion of IT Security and include both physical access to company centers, and logical access to GHS's information systems.
4. All third party personnel who require access to GHS's information resources must have a GHS director level sponsor. Access will not be granted without approval and written authorization. The sponsor will be held accountable for all activities performed by the third party.
5. Third party employees requesting access to electronic Protected Health Information must sign a Business Associate Agreement (BAA) prior to access establishment. The BAA is required whether the individual is part of a company or acting as an individual contractor. These agreements should be filed by the local center (or Corporate) sponsoring the third party.
6. When a third party service provider employee needs to be engaged for service, a blanket Non-Disclosure/Confidentiality Agreement (NDA) must be signed and maintained by the IT Project Management Organization. Execution of this NDA is required regardless of whether the work is performed is on-site or off-site. Employees of the Third Party not servicing GHS are excluded from this requirement. This agreement will address the importance of information security and must be completed prior to issuing a company badge, network accounts, or access to any company data.

7. Similarly, when there is a business need for a third party network connection, a risk assessment must be performed to determine the security implications and control requirements of the systems involved. An appropriate controls strategy must be defined and agreed upon by IT Security.
8. IT Security will obtain the appropriate records from the third party regarding their control structure for performing data processing functions or their access to sensitive information. Depending on the sensitivity and criticality of the services provided or the data accessed, the company should consider commissioning or requesting an independent review of the third party's internal control structure.
9. The GHS director level sponsor must review the business need for the third party employee and approve the request if all appropriate policies and procedures have been followed. This sponsor will be held accountable for all actions taken by the third party.
10. After completion of all prior steps in this procedure, third party employee access will be given to GHS's Internal Network and any other requested and approved information resources. If any of these steps are not fully completed and followed, the third party employee will not be granted access to GHS's information resources.
11. Vendors requiring remote access to GHS information systems will have this access provided to them on an as-needed basis. Access requests will be closely monitored to detect possible security exposures to the GHS environment.
12. External organizations are not permitted unlimited access to GHS's computers or networks. All inbound connections will be limited to specific hosts and applications on those hosts. If possible, these specific hosts and applications will be physically or logically separated from GHS's primary network.

VIRTUAL PRIVATE NETWORK (VPN)

1. Only approved GHS Workforce Members and authorized third parties (customers, vendors, etc.) may utilize VPN access. Users must abide by the ***IS-01-108: Virtual Private Networking*** policy guidelines when using VPN access.
2. By choosing to use VPN technology, third party users must be made aware that their computers are a "de facto" extension of GHS's data network, and as such, are subject to the same rules and regulations that apply to GHS-owned equipment. Refer to the GHS's ***IS-01-101 Computer Systems Acceptable Use Policy, IS-01-101A Computer Systems Acceptable Use Agreement, IS-01-114: Third Party Connection Policy and IS-01-114A: Third Party Connection Policy Agreement*** forms for more information. It is the responsibility of GHS Workforce Members, with VPN privileges, to prevent unauthorized use of their equipment and to hold confidential and protect all sensitive information including their account username and password. All computers connected to the GHS data network, via VPN, must use the most up-to-date corporate standard anti-virus software. Users requesting VPN access must provide the type of anti-virus software as well as the version of the virus definition table (DAT) file currently used.

SANCTIONS AND VIOLATIONS

Any GHS Workforce Member found to have violated this policy may be subject to disciplinary actions, up to and including discharge from employment, civil penalties, criminal prosecution, and the ability to do business with GHS.

CONTACT INFORMATION

If you have questions regarding this policy, please contact GHS Information Services Department at 404-616-1700.

DEFINITIONS / GLOSSARY

Computer Systems: Including but not limited to computers, network, Internet connections, telecommunications system, USB drives, routers, switches, wireless access points, PDAs, software applications and email systems.

Critical Application: A GHS financial application that has materiality, impact, or control over GHS's financial reporting position.

GHS Workforce Members: Employees, medical staff, interns, visitors, contractors, students, volunteers, Business Associates, or other member which is engaged with GHS

Grady Health System: Grady Memorial Hospital, associated clinics, and Crestview Nursing Home

HIPAA: The first comprehensive Federal protection for the privacy of personal health information

Third Party Organization: Any external company from which GHS purchases products and/or services.

VPN: A process by which a data packet is encapsulated using a defined encryption algorithm, delivered to a target device, and decrypted to recover the original data packet. This process is referred to as a "tunnel" over an insecure data network and prevents unwanted parties from seeing the original information during transportation.

ACRONYMS

Acronym	Definition
GHS	Grady Health System
ePHI	electronic Protected Health Information
HIPAA	Health Insurance Portability and Accountability Act
IT / IS	Information Technology / Information Services
VPN	Virtual Private Network(ing)

REFERENCE

Joint Commission Standards: *IM.02.01.01*

Joint Commission Standards: *IM.02.01.03*

GHS Computer Systems Acceptable Use: *IS-01-101*

REVIEWS AND APPROVALS

The review and approval administrative document is maintained and stored by the Information Services Department.

HEALTHCARE PROVIDER DISCLAIMER

GHS has developed these policies and procedures in conjunction with administrative and clinical departments. These policies and procedures should not be construed as dictating exclusive courses of treatment and/or procedures. No healthcare team member should view these documents and their bibliographic references as a final authority on patient care. Variations from these policies and procedures may be warranted in actual practice based upon individual patient characteristics and clinical judgment in unique care circumstances.