GBUAHN Privacy and Security

Patient Rights and Responsibilities: Physical and Electronic Access

The organization has implemented a company-wide process for managing physical and electronic access to sensitive information, including:

1. Protections for physical facility access.
It is GBUAHN policy that security systems are in place and operational at all GBUAHN participating provider locations and that video surveillance is utilized onsite.

2. Protections for electronic access.
GBUAHN has written policies and procedures to address electronic access to patient protected health information (PHI) throughout the organization. It is GBUAHN policy that all providers, suppliers, participants, participant employees, administrators and contractors sign and comply with the Centers for Medicare & Medicaid Services (CMS) Data Use Agreement. By signing this agreement, all users agree to ensure the integrity, security and confidentiality of GBUAHN patient PHI.

3. Media and device controls.
GBUAHN participating providers are required to mitigate potential privacy risks at workstations by utilizing privacy screens for desktop computer monitors, BitLocker technology on all computer systems including laptops, inactivity timeout, key-locking desks, and to limit information displayed on electronic whiteboards and other computer screens which may be visible in public areas.

4. Physical safeguards for workstations.
GBUAHN participating providers are required to mitigate potential privacy risks at workstations by utilizing privacy screens for desktop computer monitors, BitLocker technology on all computer systems including laptops, inactivity timeout on computer systems, locking desks, and to limit information displayed on electronic whiteboards and other computer screens which may be visible in public areas, and to utilize video surveillance in offices whenever possible. In addition, access to building floors is restricted through the use of an electronic FOB system. Access is granted and controlled by GBUAHN's COO.

5. Procedures for allowing and removing access according to role-based employment.
GBUAHN participating providers are required to mitigate potential privacy risks at workstations by utilizing privacy screens for desktop computer monitors, BitLocker technology on all computer systems including laptops, inactivity timeout on computer systems, locking desks, and to limit information displayed on electronic whiteboards and other computer screens which may be visible in public areas, and to utilize video surveillance in offices whenever possible.