goldstar pediatrics

SECURITY POLICY STATEMENT

Purpose: The following security policy is adopted to ensure that Goldstar Pediatrics complies appropriately with applicable federal and state security protection laws and regulations. Protection of electronic protected health information (*e*PHI) is of great importance to this Physician Practice. Violations of any of these provisions will result in appropriate disciplinary action including possible termination of employment.

Effective Date: This policy is in effect immediately consistent with the enactment of applicable laws and regulations as of September 23, 2013.

Expiration Date: This policy remains in effect until superseded or cancelled.

Assigning Privacy and Security Responsibilities
It is the policy of Goldstar Pediatrics that specific individual(s) within our workforce are assigned the responsibility of implementing and maintaining the HIPAA Privacy and Security Rule's requirements. Furthermore, it is the policy of Goldstar Pediatrics that these individual(s) will be provided sufficient resources and authority to fulfill their responsibilities.

Risk Analysis
It is the policy of Goldstar Pediatrics that a risk analysis has been completed and is periodically updated to assess potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI. It is the policy of Goldstar Pediatrics that the risk analysis includes a review of the critical nature of electronic PHI and related applications or business processes with a subsequent ranking or prioritization (criticality analysis).

Risk Management
It is the policy of Goldstar Pediatrics that security measures are in place and maintained sufficient to reduce risks and vulnerabilities to reasonably appropriate level to:
1) Ensure the confidentiality, integrity and availability of all electronic PHI that this Physician Practice creates, maintains, stores, or transmits;
2) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI;
3) Protect against any reasonably anticipated uses or disclosures of electronic PHI that is not permitted by HIPAA or applicable state law; and
4) Ensures that all members of the workforce are aware of these requirements and comply with them.

Sanctions
It is the policy of Goldstar Pediatrics that sanctions will be applied to workforce members who fail to comply with the security policies and procedures.

Rev 02/23/2016

Information System Activity Review
It is the policy of Goldstar Pediatrics that information system activity records are regularly reviewed such as security incident tracking reports.

Supervision
It is the policy of Goldstar Pediatrics that an authorized, knowledgeable person must supervise maintenance personnel whenever work is being done on a system that contains or processes electronic PHI. It is also the policy of this Physician Practice that access authorization for maintenance personnel must be set appropriately for the jobs assigned to each.

Personnel Clearance
It is the policy of Goldstar Pediatrics that personnel be cleared before access to electronic PHI is allowed.

Personnel and Workforce Termination
It is the policy of Goldstar Pediatrics that personnel and workforce will have all access to electronic PHI terminated as soon as practicable after they are terminated. This will include physical access to our facility as well as technical access.

Training and Awareness
It is the policy of Goldstar Pediatrics that all employees and contractors receive training in security awareness and in the security procedures to be followed during the performance of their duties. It is the policy of Goldstar Pediatrics that periodic reminders and training will be provided to the workforce.

Protection from Malicious Software
It is the policy of Goldstar Pediatrics that it will implement and maintain procedures for detecting, reporting and guarding against malicious software. It is the policy of Goldstar Pediatrics that all members of the workforce will be periodically reminded and trained regarding this policy. While using Goldstar Pediatrics' email or computer devices, all employees will protect against viruses and malicious codes by: (a) Never opening or downloading any files attached to an email from an unknown or suspicious source; (b) Deleting spam and other junk email as soon as practicable; and (c) Contacting the Privacy Officer immediately if an employee suspects a virus or other suspicious activity.

Log in Monitoring
It is the policy of Goldstar Pediatrics that log in attempts and discrepancies will be monitored to the extent practicable.

Password Management
It is the policy of Goldstar Pediatrics that a written procedure will be followed to create and assign passwords, which will include periodic changing and safeguarding of passwords. All employees are prohibited from sharing their passwords and each employee must ensure that others cannot learn his/her password. Passwords must not be stored where it may be easily accessible by others.

Rev 02/23/2016

Security Incident Policy
It is the policy of Goldstar Pediatrics that all security incidents (suspected or actual) will be identified and an appropriate response developed, including but not limited to documentation in writing. Any harmful effects or violations will be mitigated to the extent practicable. All responses and follow up actions will be documented.

Breach Notification Policy
It is the policy of Goldstar Pediatrics that upon discovery of an actual or suspected breach of unsecured protected health information, this Physician Practice will follow all standards and implementation specifications to investigate the breach. This includes conducting an internal risk assessment to determine if a breach has occurred, and to assess if the breach compromises the security or privacy of the protected health information (is a violation of the HIPAA Privacy Rule) and poses significant risk of financial, reputational, or other harm to the individual. Based on this internal risk assessment and determination that the breach is not an excepted circumstance, this Physician Practice will provide prompt notification (and in no case delay the notification beyond time periods allowed by law) to affected individuals; based on the number of affected individuals and other breach characteristics this Physician Practice will (where applicable) also post notification on its website, maintain a toll free number for inquiries and questions, notify prominent media and notify the Secretary of the Department of Health and Human Services. All notifications will be made in plain language and with content as required by law. This Physician Practice will maintain documentation of all investigation and documentation of breaches. This Physician Practice will revise and maintain procedures and agreements with its business associates consistent with this Breach policy and sufficient to contractually require prompt investigation, notification and cooperation by the business associate. This Physician Practice will maintain workforce training, sanctions, and whistleblower protections related to this Breach policy. This Physician Practice will remediate any gaps in compliance and systems to secure PHI as soon as practical after these are discovered. This Physician Practice will ensure that all Breach notification requirements mandated by State law are also followed.

Contingency Plans
It is the policy of Goldstar Pediatrics that a contingency plan is in place and maintained. The contingency plan includes procedures for data backup, disaster recovery including restoration of data, and emergency mode operations. It is the policy of this Physician Practice that the contingency plan includes a procedure to allow facility access in support of restoration of lost data and to support emergency mode operations in the event of an emergency. It is the policy of this Physician Practice that access control will include procedures for emergency access to electronic PHI.

Testing
It is the policy of Goldstar Pediatrics that all security controls and measures in place be periodically tested to ensure proper functioning. It is also the policy of this Physician Practice that all procedures adopted to protect the confidentiality, integrity and availability of information and information services be tested to ensure that important security considerations have not been overlooked. It is also the policy of this Physician Practice that contingency plans and related measures will be periodically tested to ensure proper functioning and to maintain readiness in the event of a contingency.

Rev 02/23/2016

Evaluation
It is the policy of Goldstar Pediatrics that a periodic technical and non-technical evaluation will be conducted to audit the effectiveness of the security controls and measures in place in consideration of environmental or operational changes.

Audit
It is the policy of Goldstar Pediatrics that audit controls are in place to record and examine the activity of all information systems that contain or use electronic PHI. This Physician Practice will maintain procedures to protect electronic PHI from improper alteration or destruction and to routinely authenticate that electronic PHI retains its integrity (including but not limited to version control, read only privileges).

Authentication
It is the policy of Goldstar Pediatrics that all information system users be authenticated before access to information processing resources is allowed. Specifically, each user must have his or her own system account, and passwords must never be shared.

Authorization and Termination
It is the policy of Goldstar Pediatrics that authority to access electronic PHI be granted or supervision be provided to users who will work with electronic PHI. When these users no longer require their access or are terminated, all authorization will cease including the revocation and deletion of passwords, user ID's and system privileges.

Access to Protected Health Information
It is the policy of Goldstar Pediatrics that all access control mechanisms must be configured to allow access only to the information and information processing functions needed by each employee or contractor to perform their assigned duties. It is also the policy of this Physician Practice that proper procedures must be followed whenever access to health information is authorized, established or modified and that records of access authorizations must be maintained. Access will be granted and maintained to the extent possible at a system level, role or job function (and application software) level, and workstation or device level. It is the policy of this Physician Practice that access control will include unique name/and or numbers to identify and track user identity. It is the policy of this Physician Practice that access controls will include automatic log offs for unattended computer sessions and, as appropriate, applicable encryption of electronic PHI (including system level encryption for stored data, and stored data on other devices such as workstations, portable devices and backup media). It is the policy of this Physician Practice that appropriate password protection will be implemented. It is the policy of this Physician Practice that emergency access will be maintained by relying on a backup list of user IDs and passwords.

Device and Media Access Control
It is the policy of Goldstar Pediatrics that reusable media, such as tapes, zip disks or diskettes, or hardware that contains electronic PHI must be securely erased or otherwise destroyed before being discarded to prevent unauthorized access to electronic PHI. This policy extends to media that will be reused by another party. It is the policy of this Physician Practice to safeguard and account for the receipt and removal of all hardware and media containing electronic PHI. It is the policy of this Physician Practice to backup devices that contain critical electronic PHI or applications prior to their relocation as appropriate.

Physical Access Control
It is the policy of Goldstar Pediatrics to limit physical access to electronic information systems (including diagnostic equipment that maintains electronic PHI) to those properly authorized. It is also the policy of this Physician Practice that appropriate safeguards are in place to protect these systems and the electronic PHI they contain from tampering, theft or destruction. It is the policy of this Physician Practice that visitors sign in and are verified and monitored. It is the policy of this Physician Practice to review and supervise any repairs or modifications to the facility that could compromise security.

Workstation Use Guidelines
It is the policy of Goldstar Pediatrics that workstations be positioned in such a manner as to avoid accidental, unauthorized exposure of health information. It is the policy of this Physician Practice that displays be locked when unattended. It is the policy of this Physician Practice that access to workstations is restricted to authorized users. This workstation policy extends to desktop computers, laptop computers, PDA's, electronic diagnostic equipment and all storage media connected or stored in the immediate environment. Users of mobile devices must protect against inadvertent and unauthorized disclosure of electronic PHI through the device. Particular care is needed when traveling and at home to protect and secure such devices.

Secure Data Transmission
It is the policy of Goldstar Pediatrics that data communications that contain electronic PHI must be encrypted or transmitted using a secure transmission protocol if they traverse public networks such as the Internet. It is also the policy of this Physician Practice that all data transmission methods must incorporate data integrity and authentication controls. Any transmission of data using mobile devices must be done through secure transmission protocol.

Configuration Management
It is the policy of this Goldstar Pediatrics that proper procedures be followed for the installation or removal of all hardware devices or software programs. It is also the policy of this Physician Practice that the hardware/software inventory must be kept current and that the configuration must be documented in sufficient detail to be rebuilt in the case of an emergency.

Business Associates
It is the policy of this Physician Practice that business associates must comply with the HIPAA Privacy and Security Rules to the same extent as this Physician Practice, and that they be contractually bound to protect health information to the same degree as set forth in this policy pursuant to a written business associate agreement. It is also the policy of this organization that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate, or if that is not feasible, by notification of the HHS Secretary. Finally, it is the policy of this organization that organizations that transmit PHI to this Physician Practice or any of its business associates and require access on a routine basis to such PHI, including a Health Information Exchange Organization, a Regional Health Information Organization, or an E-prescribing Gateway, and Personal Health Record vendors, may be business associates of this Physician Practice.

Rev 02/23/2016

S.B.1386 and A.B.1298 Compliance
It is the policy of Goldstar Pediatrics that it will comply with state laws regulating the response to any breach of unencrypted information that could be used for identity theft or other malicious activities.

Document Retention, Availability and Currency
It is the policy of Goldstar Pediatrics that these policies and all related procedures be retained for 6 years from the date of its creation or the date when it was last in effect, whichever is later. It is also the policy of this Physician Practice to make this documentation available to those persons responsible for implementing the related procedures and that this documentation and policy will be kept current in response to relevant environmental or operational changes or changes in law.

Investigation and Enforcement
It is the policy of Goldstar Pediatrics that in addition to cooperation with Security Oversight Authorities, this Physician Practice will follow procedures to ensure that investigations are supported internally and that members of our workforce will not be retaliated against for cooperation with any authority. It is our policy to attempt to resolve all investigations and avoid any penalty phase if at all possible.

Personal Internet Accounts
It is the policy of Goldstar Pediatrics that all employees are prohibited from using any personal email accounts and internet connections, including but not limited to instant messaging, Facebook or Twitter, for communicating messages containing PHI.