| | |
|---|---|
| **DEPARTMENT:** Information Protection and Security | **POLICY DESCRIPTION:** Pediatric Security Program |
| **PAGE:** 1 of 9 | **REPLACES POLICY DATED:** 10/1//20, 9/1/23 |
| **EFFECTIVE DATE:** July 1, 2024 | **REFERENCE NUMBER:** IP.PS.007 |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

**SCOPE:** All Company-affiliated hospitals and free-standing emergency departments.

**PURPOSE:** To provide the physical safety and security framework for the pediatric patient.

**POLICY:**

A. Each Company-affiliated hospital that provides pediatric care will promote the security of pediatric patients. Pediatric security should include a whole-facility approach. Physical security, written protocols, policies, and procedures, as well as staff education and training, should be seamlessly interfaced with campus, facility, and unit security, as well as the local community law enforcement, to provide total security integration. Additionally, every child reported missing within the campus, meaning the whereabouts are unknown to those responsible for their well-being, will be considered at risk until significant information to the contrary is confirmed.

B. Access to designated Pediatric care units will be limited.

C. ID Badge compliance on the Pediatric units will be strictly enforced at the facility

D. Facility will comply with company technology standards related to pediatric security.

**PROCEDURE:**

A. Gap Assessment *PD, IP, OS, ER (see Legend pg. 8)*
   1. Annually, or when significant changes occur to areas where pediatric patients receive care, the facility Security department will lead the effort to complete a self-assessment and develop a gap analysis with an action plan based on findings. The facility will ensure the gap assessment is uploaded into Complyos.
   2. The action plan will be presented to the facility's Environment of Care Committee. The committee will continuously track open action items until resolved.

B. Training *PD, IP, OS, ER*
   1. Pediatric security-specific training for all facility colleagues is completed during new hire orientation.
   2. Additional security training for colleagues involved in the direct care of pediatric patients is to be completed prior to or during the employee's first shift in the patient care area. Refresher training will occur annually.

C. Pediatric Security Assessment *PD, IP, OS, ER*
   1. During the initial assessment/encounter the patient/parent/guardian will be asked if there is any personal circumstance the facility should be aware of, especially as it relates to a family situation that might place the parent/guardian or child at-risk.
      a. Examples of Risk factors refer to a child:
         1) 13 years of age or younger;

2) Involved with child and/or adult protective service;
3) Involved in a custody dispute;
4) Suicidal, runaway or elopement history;
5) Out of the zone of safety for their age and developmental stage. Zone of safety refers to cognitive deficits and an individual's mental processes (e.g., knowledge, judgement, and reasoning) that lead to the acquisition of information and drive how an individual understands or acts in the world;
6) With mental or behavioral disabilities;
7) Cognitively impaired (medications, anesthesia, dementia);
8) On emergency detention;
9) In the company of others who could endanger their welfare;
10) Behavioral patterns are inconsistent with their normal behavior and the change cannot be readily explained; or
11) Is involved in a situation causing a reasonable person to conclude the patient should be considered at risk.

b. If a patient has one or more of the above risk factors, the following response and interventions will be assessed:
1) Making patient confidential and/or "no information" status;
2) Moving patient in closer proximity to the nursing station within sight of the nursing staff and increasing nursing surveillance;
3) Need for increased frequency of observation;
4) Need for a sitter;
5) Family's willingness to provide support;
6) Posting a description and/or pictures of people to watch out for at the nursing station;
7) Posting a security guard and/or safety attendant at the patient's room or on the unit; or
8) The admitting nurse will ask the patient/parent/guardian to identify, in writing on the Pediatric Security Education form, who may accompany the patient outside of the room. *PD, IP*
9) When transporting a patient, specifically state in the hand-off that this patient is considered "at-risk" and the nature of the risk (i.e., abduction, elopement or harm to themselves).

D. Designated Pediatric Care Units *PD*

1. Physical Environment Security
    a. Proximity locks with a badge or card swipe access is required on department perimeter doors, including elevators and stairwells.
    b. Access codes to units where pediatric patients are located are changed at irregular intervals and at least annually.
    c. Entry and exit doors will be secured 24 hours a day, 7 days a week. Emergency exit doors will have a delayed egress function activated per local fire code/Marshall.
    d. Doors will include an audible door alarm function. The audible alarm will be locally sounded, as well as at centralized locations.
    e. Pediatric units should minimize the number of times the pediatric patient is removed from the room or a staff-supervised unit.
    f. Pediatric unit colleagues should perform random security checks throughout the shift (i.e., checking empty rooms, badges, security of doors, etc.).
    g. Empty or unoccupied patient room doors should be left open at all times unless the Fire Marshall or Authority Having Jurisdiction (AHJ) requires otherwise. If doors are equipped with a self-closing mechanism, their operation must not be impeded by devices such as manual hold open devices, furniture, wedges, etc. Self-closing doors should be equipped with automatic hold open devices that are of appropriate design and connected to the fire alarm system, which ensures closure upon activation of the fire alarm. In the event of a fire, empty or unoccupied patient room doors should be closed.
2. Colleague Access
    a. Only clinical and non-clinical colleagues that conduct routine business within the department should have electronic access to the department. Access is to be reviewed on an annual basis by the facility security department and hospital leadership.
    b. Colleagues that resign from the unit will have their access revoked immediately after their last shift. Access (add, modify, delete) will be requested following the facility process (i.e. Electronic Security Access Form (eSAF), Human Resources or Security).
3. ID Badges
    a. Facility will control and inventory process for issuance, tracking, and subsequent retrieval of hospital-issued, unit-issued, permanent and/or temporary distinctive ID badges.
    b. Pediatric unit distinctive ID badges, including individuals that are allowed to transport pediatric patients, will be turned in upon termination, resignation, or when the individual is no longer associated with the facility.

c. Temporary-issued ID badges issued to students or contractors, etc., are returned to a designated facility individual at the end of shift, contracted work hours, etc.

d. All ID badges will be worn visibly on the chest area to ensure the picture, name, and facility logo are facing outward and unobstructed by pins, decals, or other devices (i.e., double-sided badges or a stationary badge may be used).

e. Colleagues providing patient care that may involve transporting pediatrics (including agency and traveling nurses) are required to have a distinctive, facility-issued Pediatric unit badge to identify them as a member of that unit and having the authority to transport.

f. Colleagues, including administrative and ancillary staff, presenting on the Pediatric unit(s), are required to wear a facility-issued photo ID badge.

g. Pediatricians, Advanced Practice Clinicians and Licensed Independent Practitioners providing pediatric patient care are required to have a distinctive, facility-issued ID badge.

h. Ancillary and support colleagues will be expected to wear a facility-issued ID badge and are required to notify unit staff of the purpose for presence on the unit.

i. Students and Contracted Staff (i.e., audiology services, photography services, etc.) providing additional healthcare services are required to wear an accompanying school/company ID badge and will be provided with a temporary unit-issued badge with agreeing facility logo indicating unit access permission per facility policy.

j. Non-healthcare service providers (i.e., consultants, vendors, etc.) are required to wear an accompanying company ID badge and will be provided with a temporary facility-issued badge with agreeing facility logo indicating facility access permission per facility policy.

4. Unit-Specific Colleague Uniforms

a. Pediatric unit colleagues are required to wear unit or facility-specific attire according to their facility's dress code policy.

b. There will be a control and inventory process for issuance, tracking, and subsequent retrieval of facility-issued, unit-issued permanent and/or temporary distinctive uniforms, patches, etc., for the Pediatric units.

c. Facility-owned pediatric specific scrubs that are stored on site are kept in a secured environment with access limited to unit colleagues and other essential personnel with processes to manage inventory. Visitor and vendor scrubs are distinctive and are disposed of or returned at the end of each visit.

5. Inpatient Behavioral Health Units

a. Parents/Guardians are not required to stay with the patient and do not need to identify in writing who may accompany the patient outside the room.

b. Empty or unoccupied patient room doors should be closed and locked to prevent entry as a security measure.

c. The number of times the pediatric patient is removed from the room is determined by their specific treatment plan/needs.

d. The behavioral health unit colleagues will participate in facility-wide quarterly drills. Each facility should determine the appropriateness of initiating drills from the Pediatric behavioral health units.

e. Exemptions for the above requirements should be based on a facility-specific risk assessment.

6. Electronic Pediatric Security System *PD*

a. If the facility has an electronic pediatric security system, application of the electronic security device should be applied upon admission to the Pediatric Unit.

b. If the facility has an electronic security system, activation of the electronic security device takes place at the moment the patient is within the security zone when conditions allow.

c. If the facility has an electronic security system and removal and/or deactivation of the electronic security system device is required at time of discharge, the child will remain supervised while on the unit by authorized colleagues wearing the authorized Pediatric distinctive badges and uniform using direct, line-of-sight supervision until physically discharged from the facility. Upon discharge, electronic security devices should be removed immediately prior to exiting the pediatric unit.

d. If the facility does not have an electronic security system, or application and/or activation of the electronic security system device is delayed due to physical plant or system default, the pediatric patient will be transported by authorized colleagues wearing the authorized Pediatric distinctive badges and uniform using direct, line-of-sight supervision.

e. The Security Administrator or designee will be responsible for:
   1) maintaining and fixing the electronic pediatric security system;
   2) testing equipment on a monthly basis (uploaded into Complyos); and
   3) reviewing event and alarm reports to mitigate risks. Events and Alarms to be activated and tracked are:
      i. Tag exit alarm (Security)
      ii. Tag cut/tamper (Security)
      iii. Tag at exciter (Security)
      iv. Improperly applied tag (Procedure)

f. Security events/alarms should be minimal in occurrence and will be reviewed in detail by security and unit leadership. Investigations will be presented to the Environment of Care Committee.

g. At least quarterly, technology should be evaluated for the propensity of false alarms and dead spaces. The evaluations should occur through a collaborative effort involving facility engineering, security, information technology, and nursing management.

h. In the event electronic security systems (i.e., badge access, electronic patient security tags, remote door releases, etc.) experience downtime or temporary malfunction, application of physical controls and safeguards (i.e., clinical colleagues informing parents and elevated security needs) should be implemented immediately.

E. Pediatric Identification *PD, IP, OS, ER*

1. Application of parent/guardian identification bands upon admission/arrival, or as soon as safely possible.
2. Facilities that obtain a photograph or video/digital image of the pediatric patient as part of their security process should obtain the image upon admission.

F. Visitors *PD, IP*

1. The admitting nurse will ask the patient/parent/guardian to identify, in writing, visitors who are restricted from visitation. This list is to be part of the medical record until discharge and updated, as needed. Visitor restrictions should be included in handoff communication.
2. Pediatric Inpatient Units will have a process for visitor identification (e.g., visitor log book, visitor ID validation, visitors receive a distinctive visitor wristband or name tag allowing entry to the unit, etc.). The visitor wristband should be a cut-away, non-transferable, disposable band with no patient identification.
3. Vendor access will be restricted and allowed only for necessary patient care and safety. Vendor credentials will be verified, and vendor access will be renewed each day.
4. External vendors and/or agency representatives who are required to interact with pediatric patients and/or parents need to be appropriately identified upon arrival to the unit and introduced to the parents/guardians by the primary care nurse.

G. Additional Security Measures for Outpatient Services *OS, ER*

1. All pediatric patients should be accompanied by a parent/guardian.
2. At no time should a pediatric patient be left alone without supervision by a parent and/or guardian, except if a medical procedure prohibits this. During medical procedures, facility colleagues will remain with the patient at all times.
3. In the event a pediatric patient is left unsupervised, an attempt shall be made to contact the parent(s) and/or guardian immediately. If the parent(s) and/or guardian cannot be located in a reasonable amount of time, the supervisor, facility security and/or case management shall be contacted.

H. Parent/Guardian Education

1. Parents/guardians will be educated on security awareness, identification of facility personnel, primary care colleagues for the shift, and communication regarding unit activities and any procedures involving the pediatric patient.
2. Parents/guardians should sign a form acknowledging an understanding of pediatric security education provided and shared responsibility for maintaining pediatric security during facility stay. Documentation will be included in the patient's medical record.
3. Language and cultural barriers may interfere with the understanding of, or compliance with, pediatric security education. Therefore, efforts should be made to achieve optimal understanding by the parent/guardian and documented in the medical record. *PD, IP*
4. Home Care education will include: *PD, IP, OS, ER*
   a. Vendor/agency name;
   b. Purpose of visit;
   c. Anticipated arrival;
   d. Expected vendor and/or agency representative identification; and
   e. Advisory to parents/guardians to remain present with the child in the home during the vendor/agency representative's visit.

I. Discharge Procedures *PD, IP, OS, ER*

1. Release pediatric patients after the patient and the parent/guardian ID bands are validated.
2. If no ID band is available, colleagues are to validate with government-issued picture ID.

J. Pediatric Abduction-Drills, Potential and Actual *PD, IP, OS, ER*

1. The Patient Safety Director will be responsible for validating that pediatric abduction drills are completed in partnership with security and unit leadership. In all facilities, pediatric abduction drills should involve the entire campus and be conducted at a minimum of one per quarter. Drills are to be conducted at varying times to include all shifts and should not establish a predictable pattern. Drills should be initiated where Pediatric care is provided using a realistic scenario with critique. All critiques, findings, and action plans should be reviewed by the Environment of Care (EOC) Committee for oversight. The facility will ensure completed drills are uploaded into Complyos.
2. Potential Abduction: Facility colleagues should be alert to any unusual behavior they encounter from individuals. The alert process should include the recommendations provided by the National Center for Missing and Exploited Children and generate a communication and action plan based on observation and findings.
3. Actual Abduction: To assist in the timely identification of an abducted patient and/or an abductor, the facility response for pediatric abduction includes:

a. Activating the facility pediatric abduction alert.

b. Performing a facility-wide overhead page notification, which should include the location from which the child was abducted, gender and age, a description of the child, and a description of the abductor, if available. The announcement will occur every two minutes until an "all clear" is initiated.

c. Security responding to the location of the reported abduction shall sequester the area, moving family from the current location to another secure area.

d. Colleagues immediately responding to stop vertical (floor to floor) movement, by securing interior departments, stairwells and exterior doors, allowing only designated individuals (i.e. Law Enforcement, Security and/or Senior Leadership) to have unfettered access.

e. Designating specific individuals that may cancel the security alert. Facility may choose to utilize a special passcode to validate individuals.

f. Having a designated representative responsible for communicating with Law Enforcement agencies, relaying and updating information, as well as receiving communication from Law Enforcement for further instructions.

**DEFINITION:**

**Abduction** The action or an instance of forcibly taking an individual away against their will.

**Alarms** Notification that the system has triggered and/or reached the second designated limit.

**Dead space** Area that does not receive a Wi-Fi signal.

**False Alarm** Alert activated but did not actually happen.

**Pediatric patient** A person under 18 years of age who is being treated as an inpatient or outpatient.

**System Alert** Notification that the system has triggered and/or reached the first designated limit.

**LEGEND**:

**PD** Applies to Dedicated Pediatric Units

**IP** Applies to Adult Inpatient Units admitting patients under 18 years of age

**OS** Applies to Outpatient Services/Ambulatory Surgery Centers

**ER** Applies to Emergency Services

**REFERENCES:**

1. National Center for Missing and Exploited Children (2014). For Healthcare Professionals: *Guidelines on Prevention of and Response to Infant Abductions*

| | |
|---|---|
| **DEPARTMENT:** Information Protection and Security | **POLICY DESCRIPTION:** Pediatric Security Program |
| **PAGE:** 9 of 9 | **REPLACES POLICY DATED:** 10/1//20, 9/1/23 |
| **EFFECTIVE DATE:** July 1, 2024 | **REFERENCE NUMBER:** IP.PS.007 |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

2. HCA Healthcare Pediatric Security Risk *Assessment for Healthcare Facilities*
3. HCA Healthcare Identification and Name Badge policy, HR.ER.015
4. HCA Healthcare Pediatric Security Drill After Action Report template
5. Implementation Guidelines for COG.PPA.003 non-employee Dependent Healthcare Professionals (DHP's)