**Privacy and Information Security Violation Sanctions Guidelines**

**(August 8,, 2014)**

**INFORMATION:** The sanctions listed below mainly pertain to a first offense unless otherwise stated. Other performance issues, multiple or repeat offenses, or circumstances that indicate malicious intent, may result in an increase of the severity of the assigned sanctions.

**Based on the severity and risk involving any confidential or protected patient information (PHI), employee or business information, Human Resources reserves the right to adjust the severity of the assigned sanctions with supporting documentation.**

**DEFINITIONS**:

**Breach:** An “unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”

**PHI:** Protected Health Information

**Privacy:** Freedom from unauthorized intrusion.

**Significant Harm**: Having meaningful or a likely influence / threat of physical, mental, financial damage.

**\*\*** Each event may be different and will have a risk assessment completed by the System Privacy Officer or entity Privacy Site Coordinator (PSC). If it is determined that the patient could experience significant harm (reputation, financial, physical, or mental) as per the HIPAA regulation criteria, then the level of compromised PHI will be determined as “High”. A patient may also provide the assessment and consider an event significantly harmful requiring a higher level of action on ’s part.

**Unsecured PHI:** Information that is not encrypted while at rest or during transmission or the encryption standard used to secure PHI does not meet:

* National Institute of Standards and Technology (NIST) guidelines; and
* Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), a federal standard used to accredit cryptographic tools or applications.

**Willful Neglect:** A conscious, intentional failure or reckless indifference to the obligation to comply.

| **Standard Privacy/Information Security Sanctions Table - Employee** |
| --- |
| **Category or Incident Type** | **Verbal Warning and possible Privacy/IS Retraining** | **Written Warning****and Required Privacy/IS Retraining** | **Three-day Suspension or Final Written Warning and****Required Privacy/IS Retraining** | **Involuntary Termination** |
| General Overview**Column description →** **Scenarios ↓**  | **Use when incident appears unintentional, unknowing, and results in low or no harm to patient.** | **Use when breaches of Privacy or Security result in low or no harm to patient or Hospital.** | **Use when breaches of Privacy or Security result in significant harm to patient or Hospital. (may be unintentional)** | **Use when breaches of Privacy or Security results in personal gain, malicious intent, significant harm to patient, high liability to , required reporting and/or media notification**  |
| **Physical Security** Improper disposal of PHI |  | Improper disposal of PHI, no possible harm to patient or Hospital | Willful neglect in disposal of PHI low or no harm to patient or Hospital |  |
| Failure to secure **ePHI** (includes unauthorized removal of PHI from property) |  | Failure to secure either electronic or non-electronic PHI/Confidential information (low/no harm to patient/Hospital and/or no breach notification) | Willful neglect in failure to secure either electronic or non-electronic PHI/Confidential information (low or no harm to patient/Hospital and/or no breach notification) | Willful failure to secure non-electronic PHI/Confidential information (significant harm to patient/Hospital and/or breach notification) |
| **Electronic Security**Failure to sign off or lock computer | Failing to sign off or lock a given computer terminal when not in use |  | Willful neglect in failing to sign off or lock a given computer terminal when not in use (without access by another) | Allowing another user to utilize the system via his/her access code (password) resulting in wrongful access of PHI or other highly confidential employee / business information.Deliberately attempting to wrongfully access another employee’s email, files or any hospital system, including EHR.  |
| Failure to secure electronic PHI(e.g. copied to mobile media, not enabling proper access restrictions, etc.) |  | Failure to secure electronic PHI/confidential information (no risk of harm to patient/Hospital and/or no breach notification) | Willful neglect in failing to secure electronic PHI/Confidential information (low or no harm to patient /hospital and/or no breach notification) | Failure to secure electronic PHI/Confidential information (significant harm to patient/Hospital and/or breach notification) |
| **Unsecured email** | Failure to encrypt email with PHI included or as an attachment, sent to a non- network address. (low or no harm to patient) | Failure to encrypt email with PHI included or as an attachment, sent to a non- network address. (significant harm to patient) | Willful neglect in failing to encrypt email with PHI included or as an attachment, sent to a non- network address. |  |
| **ACCESS** Access own PHI |  | Willful neglect - Accessing own medical records/PHI |  |  |
| Family recordsHigh confidential, pt, empl/business info for personal gain/malicious intent |  |  | Willful neglect in accessing family members records (first offense, both PHI and specific protected information such as (Behavioral, STD, family planning, substance abuse, HIV/AIDS, etc.) and the potential for harm does exist as a result) | Accessing HIGHLY confidential PHI under false pretenses, without having a working need to do so. (Behavioral, STD, family planning, substance abuse, HIV/AIDS, etc. considered HIGHLY Confidential)Accessing, disclosing and /or amending PHI of a patient without having a job duty - reason to do so, or confidential employee/hospital information for personal /professional gain or malicious intent to sell or harm others. |
| Access patientPHI with no working need to know (includes employee/patient PHI)  |  |  | Accessing the record of a patient without having a job duty/working reason to do so (low or no harm to patient and/or no reporting required)“Snooping” (elect. Record, documents, etc.) | Willful neglect in accessing, disclosing, and/or amending PHI job duty/working reason to do so resulting in potential significant harm to patient. (Including but not limited to behavioral, STD, family planning, substance abuse, HIV/AIDS, etc.) |
| Request other user to obtain PHI |  | Request another user or employee to share (verbalize) PHI of any patient. | Requesting another user or employee to access patient information outside of his/her access ability or job duties (first offense) (elect. record, papers) |  |
| Financial / billing info of pt. |  |  | Accessing the financial or billing information of a patient without a job duty reason to do so (no significant harm to patient /guarantor and/or no reporting required.). Known as “Snooping”. | Accessing, amending, and/or using billing information of a patient without a job duty / working reason to do so and/or disclosing the information to a non covered entity (none or any potential significant harm to patient/guarantor). This would include SSN and credit card / financial information. |
| **Disclosure OR Use**Release PHI to wrong person or pt - Lack of proper ID verification |  | Unintentional - not properly verifying the patient and disclosing PHI to another party where patient identity is disclosed. (low or no harm to patient or breach notification) | Willful neglect in not properly verifying the patient and disclosing PHI to another party where patient identity is disclosed. (low or no harm to patient or breach notification) |  |
| Social Media posts |  |  | Posting information regarding patients (no names) publicly such as on social media sites which are inappropriate or the patient could be reasonably identified.  | Posting information regarding patients (no names) publicly such as on social media sites which are inappropriate or the patient could be reasonably identified with significant harm to patient.  |
| Pt. or employee pt. with significant harm |  |  |  | Accessing record of a patient (including employee pt.) without having a job duty reason to do so and/or disclosing the information to another party not involved in the patient’s care (significant harm to patient and reporting required) |
| Access/amend PHI for personal gain / malicious intent |  |  |  | Accessing, disclosing and /or amending PHI or Hospital information for personal or professional gain or intent to sell or sale of the information. |
| Discussing pt. PHI(wrongfully discussing or when overhead in an unsecure area) |  | Discussion of pt. PHI with others for work purposes yet in an area where overheard by others. (low level of harm to pt and/or no breach notification required) | Willful neglect in discussing patient care/situations with health care or other individuals without a “need to know”. (low level of harm to patient and/or no breach notification required) | Accessing, disclosing and /or amending PHI or Hospital information for malicious purposes or personal gain. |
| Leaving message | Leaving a message for a patient/parent that exceeds the minimum necessary standards (no risk of harm to patient and no reporting requirement) | Leaving a message for a patient/parent that exceeds the minimum necessary standards (second offense and no risk of harm to patient and no reporting requirement) | Willful neglect in leaving a message for a patient/parent that exceeds the minimum necessary standards (first offense, low harm to patient, no reporting requirement). May include highly confidential PHI (Behavioral, STD, substance abuse, HIV/AIDS, etc.)  |  |
| Publication or presentation PHI |  | Publication or presentation of PHI without patient authorization (low or no harm to patient) | Publication or presentation of PHI without patient authorization (significant harm to patient and breach notification). NOTE: if Research – report to IRB. |  |
| ID Theft/Fraud |  |  |  | Use of PHI for identity theft or obtaining and or using) financial information (credit card, etc.), (significant harm to patient) |
| Not properly verifying identification(e.g.: giving document with PHI to wrong person; leaving PHI message on wrong phone) | Not properly verifying individual’s identification before disclosing information, whether by phone, in person or in writing. (no harm to patient) |  | Willful neglect in not properly verifying individuals by phone, in person or in writing (low or no harm to patient and no breach notification) before disclosing information. | Willful neglect in not properly verifying individuals by phone, in person or in writing (significant harm to patient and breach notification) before disclosing information.  |
| **Data, Info Accuracy & Integrity** Registration  – wrong pt.  |  | Registration Errors – Negligence resulting in wrong patient being admitted/registered and a privacy breach (low/no harm to pt.).  | Registration Errors – Negligence resulting in wrong patient being admitted/registered and a privacy breach (significant harm to pt.).  | Intentional Registration Error – Wrong patient being admitted / registered resulting in a privacy breach and/or other legal issue.  |
| Registration –  wrong information |  | Registration Errors – Wrong pt. information documented resulting in a privacy breach (low/no harm to pt.) (PCP, contact, ins., etc.) | Registration Errors – Wrong pt. information documented resulting in a privacy breach (significant harm to pt.) (PCP, contact, ins., etc.) | Intentional Registration Error – Wrong/false pt. information documented resulting in a privacy breach and/or other legal issue |
| Misdirected fax | Misdirected Fax with PHI resulting in PHI disclosure (no harm to patient and/or no reporting required) | Misdirected Fax with PHI resulting in PHI disclosure (second offense and low or no harm to patient and/or no reporting required) | Willful neglect in misdirected Fax with PHI (significant harm to patient and/or reporting required of breach notification) |  |
| Misdirected mail |  | Misdirected mailing with PHI to another patient, person or entity in error (low or no harm to pt.) | Misdirected mailing with PHI to another patient, person or entity in error (significant harm to patient and breach notification). | Willful or intentional mailing of PHI to a wrong patient, person, or entity, resulting in significant harm to the correct patient and breach notification. |
| Altering PHI - falsification |  |  |  | Altering PHI or medical record/falsification of records. |
| **Restriction Requests**Failure to respect approved pt. request |  | Failure to respect approved patient requested restrictions with low or no harm to the patient. |  | Failure to respect approved patient requested restrictions with significant harm to patient and/or breach notification. |

**NOTE:** These guidelines support the System Privacy and Information Security Sanctions Policy.

**DEFINITION:** Workforce Members/Non-employees: persons whose conduct in the performance of work for is under the direct control of whether or not they are paid by . This includes, but is not limited to: Medical staff affiliates, Academic instructors, Students, Residents, Volunteers, Trainees, Agency personnel, Board members

|  |  |
| --- | --- |
|  | **WORKFORCE MEMBERS / NON - Employee** |
|  | In the event of a violation by a workforce member / non- employee with access to PHI software, the Chief Privacy Officer and entity Privacy Site Coordinator will work with the entity Medical Staff President and/or Chief Physician Executive, medical office manager and/or Privacy Officer of an outside entity, or company manager to assist with investigation and the appropriate sanction for that individual. Should the incident have legal involvement, personal gain, malicious intent, or resulting in significant harm to a patient, network termination, loss or suspension of staff privileges, etc. could be immediately initiated. |

**References:**

2011 – AHIMA Sanction Guidelines for Privacy and Security Violations / Breaches

**In Collaboration with:**

 Privacy Committee

 Ethics & Compliance Department

 HR Leadership

Revised: Aug. 8, 2014

New/Revisions: 9/2013, 10/2013