

Attachment C: Sanction Policy (sample)

Medical practice name: _____

It is in the best interest of the healthcare industry generally, and this practice in particular, to address the issue of securing the Privacy and Security of individually-identifiable health information in a proactive manner through implementation of sanction practice standards. Aside from the necessity to ensure patient privacy as an ethical obligation, it is smart business. Data breach notification laws in more than 40 states require an organization to notify breach victims, which can damage its reputation.

Privacy Incident categories:

The practice defines categories that define the significance and impact of the privacy or security incident to help guide corrective action and remediation.

- **Category 1:** Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge, or lack of judgment, such as a registration error that causes a patient billing statement to be mailed to the wrong guarantor.
- **Category 2a:** Deliberate unauthorized access to PHI without PHI disclosure. Examples: snoopers accessing confidential information of a VIP, coworker, or neighbor without legitimate business reason; failure to follow policy without legitimate reason, such as password sharing.
- **Category 2b:** Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain. Examples: snooper access and redisclosure to the news media; unauthorized modification of an electronic document to expedite a process.
- **Category 3:** Deliberate unauthorized disclosure of PHI for malice or personal gain. Examples: selling information to the tabloids or stealing individually identifiable health information to open credit card accounts.

Factors that may modify application of sanctions:

Sanctions may be modified based on mitigating factors. Factors may reflect greater damage caused by the breach and thus work against the offender and ultimately increase the penalty.

Examples include:

- Multiple offenses
- Harm to the breach victim(s)
- Breach of specially protected information such as HIV-related, psychiatric, substance abuse, and genetic data
- High volume of people or data affected
- High exposure for the institution
- Large organizational expense incurred, such as breach notifications
- Hampering the investigation
- Negative influence of actions on others

Factors that could mitigate sanctioning could include:

- Breach occurred as a result of attempting to help a patient
- Victim(s) suffered no harm
- Offender voluntarily admitted the breach and cooperated with the investigation
- Offender showed remorse
- Action was taken under pressure from an individual in a position of authority
- Employee was inadequately trained

Sanction process

The HIPAA regulations require that imposed sanctions be consistent across the board irrespective of the status of the violator, with comparable discipline imposed for comparable violations. This practice will enable application of general principles that will lead to fair and consistent outcomes.

Sanction implementation will follow the following steps. However, depending on the Category level of the incident, an escalated process can be followed if cause is shown:

- Documented conference with recommendations for additional, specific, documented training, if necessary
- First written warning (and training, as above, if warranted)
- Final warning, with or without suspension, with or without pay (training included, if warranted)
- Severance of formal relationship: employment, contract, medical staff privileges, volunteer status

