Sanction Guidelines for Privacy and Security Violations (2013 update) - Retired

Editor's note: This practice brief supersedes the October 2011 practice brief "Sanction Guidelines for Privacy and Security Violations."

The HIPAA Breach Notification Rule requires healthcare providers, health plans, and other HIPAA covered entities (CEs) to notify individuals when their health information is breached. In addition, breaches that affect more than 500 individuals must be reported to the Secretary of Health and Human Services and the media. Under the Health Information Technology for Economic and Clinical Health Act (HITECH), the HHS secretary is required to post a list of these breaches on the department's website, which is available at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

As a result of these regulations, media reports of healthcare privacy and security breaches continue to increase in number and scope. These reports threaten efforts to build consumer trust in electronic health records (EHR), health information exchange (HIE), and healthcare reform.

They also reveal a wide range of provider philosophies and responses regarding breaches. Healthcare organizations have differing access management controls, enforcement policies, and employee sanctions. For example, in one case, an employee reviewed a record they should not have and got fired. In another, a physician lost a USB device with 1,000 patients' information on it and underwent counseling. In addition, organizations caught in the media spotlight have shown varied readiness to address the press with a solid and serious message that embraces their privacy and security responsibilities.

The stakes are raised under HITECH enforcement and the potential for harm to an organization has increased greatly.

Organizations must ensure that workforce sanctions related to HIPAA privacy and security violations are relevant not only to the incident but also to the potential for compromise of the PHI that was breached. In addition, they must ensure sanctions are developed and standardized to complement and support all applicable organizational human resources and professional staff corrective action policies and processes.

This practice brief is intended to bring awareness for a united industry message of the seriousness regarding the handling of violations by workforce members. This brief offers methods for sanction management within organizational policies. This guidance mirrors the breach category approach now codified by HITECH, which encourages sanctions fitting to breach motivation, whether civil or criminal in nature.

Federal and State Breach Regulations

The greatest threat to privacy and security rests within an organization's workforce. In an attempt to hold organizations accountable, federal and state laws have mandated breach prevention and penalties. These are becoming more stringent.

While HIPAA's privacy and security rules establish a national floor for confidentiality, CEsare encouraged to develop their own internal enforcement and sanctioning approaches to meet overall compliance. Variation in EHR functionality and controls increases the likelihood that organizations adopt disparate safeguard approaches.

Some states have passed legislation tightening privacy controls within their geographic area of influence, including private right of action. These laws create even wider gaps in national enforcement and sanctioning experiences.

This past patchwork of legislation and practice was met in 2009 with data breach provisions in the HITECH Act, part of the American Recovery and Reinvestment Act (ARRA). Acting in tandem with the 2013 revised HIPAA Final Omnibus Rule, the law's expanded and direct breach accountabilities at the individual and business associate levels place profound administrative responsibility on healthcare organizations and, as recent penalties attest, threaten life-changing enforcement on perpetrators—internal workforce members, contractors, and external players alike.

All healthcare organizations face the same charge: to uphold the confidentiality of the health information they create and maintain. Privacy and security professionals have a direct impact on building consumer trust by showing firm leadership on consistent policy enforcement and sanction application for privacy and security noncompliance.

Importance of Practice Guidelines for Privacy and Security Sanctions

The disparity among organizational responses to employee privacy and security violations has a far-reaching impact on the healthcare industry. Consequences include the following:

Confusing message. An inconsistent organizational response to a violation sends a confusing message to both staff and the public. Healthcare workers moving from one organization to another find differing tolerance levels for the same actions.

Inconsistent corrective disciplinary actions. Organizations have reported terminating some staff while issuing lesser reprimands or suspensions to higher-level staff for the same type of offense. Staff may interpret this to mean that it is acceptable to breach privacy or security rules as long as an individual holds a certain status in the organization. The healthcare industry should nurture an image of solidarity in enforcing the privacy and security of protected health information (PHI) in a standardized approach across the workforce, from file clerks to medical staff members. It is important to maintain standardization across larger health systems with clear documented sanction guidelines.

Poor compliance. Staff in organizations with less stringent enforcement may weigh the level of risk to themselves against the potential advantages; for example, taking home PHI in order to catch up on work over the weekend. Staff members who perceive a lower risk may ignore security and privacy policies designed to protect PHI. Inequity in sanction application encourages poor compliance by individuals who know they will escape serious consequences for breaching privacy and security policies.

Delayed response in applying sanctions. A delayed response to a violation might imply a lack of commitment to protecting patient privacy. Delays in applying sanctions place the organization at risk, allowing security risks and violations to go unaddressed. Sanctions must be prompt and suitable to the severity of the violation so that employees understand the organization is serious about information privacy and security enforcement.

Erosion of public trust. Public trust is eroded when significant variation is blatantly apparent in how healthcare organizations prevent and manage privacy or security violations both within and across entities and systems. The public must feel assured their PHI has sufficient protections across the healthcare spectrum, particularly in this era of HIE.

Weakened position for dispute resolutions. Inequitable application of sanctions can affect the outcome of personnel actions at arbitration and grievance proceedings. Unequal penalties for similar offenses undermine the organization's ability to prevail in dispute resolutions.

Vulnerability to civil actions and lawsuits. Healthcare organizations leave themselves open to both individual and class action lawsuits when they do not have a strong, consistent privacy and security compliance program. Under HITECH, state attorneys general are now authorized to bring civil suits against CEs on behalf of individuals. The Office for Civil Rights (OCR) has funded training for attorneys general on how to bring these suits forward. This new provision strengthens the capabilities of the states and empowers OCR's overall enforcement.

Vulnerability to penalties and fines. OCR will continue to increase its enforcement activities, and the federal judiciary is becoming engaged in enforcing privacy and security violations and imposing ever-increasing fines. Inconsistent application of sanctions at the organizational setting may affect how OCR and the federal judiciary view such issues.

More regulation. Poor and inconsistent implementation of privacy and security safeguards invites further state and federal intervention. States have imposed more stringent reporting obligations and stiffer penalties on healthcare organizations, business associates, and individuals. Such laws place an additional administrative and financial burden on organizations. If the industry does not self-correct, then it leaves open the door to state and federal government intervention. HITECH has brought to light federal intervention by requiring regular privacy and security audits as a measure of OCR's enforcement.

Research integrity. The validity of research may be called into question when privacy or security violations are not handled consistently and expeditiously. Patients are less likely to participate in research studies with an organization that has an inconsistent sanction policy for privacy and security breaches.

It is in the organization's best interest to address these privacy and security compliance issues in a proactive manner through development and agreement on sanction practice guidelines. Aside from the necessity to ensure patient privacy as an ethical obligation, it is smart business. Failure to do so may result in harm to the patient as well as the organization. Data breach notification laws in most states require an organization notify breach victims, which can damage its reputation.

Sanctioning Models

Healthcare organizations should categorize sanctions according to the nature of the privacy or security incident. Categorization helps standardize corrective action determinations, assists with trending privacy and security violations, and makes reporting easier. Two models are depicted below:

Model 1—Categories of Privacy and Security Incidents

In the first model, an organization creates categories defining the significance and impact of the privacy or security incident to help guide its corrective action and remediation steps:

- **Category 1: Accidental or inadvertent violation.** This is an unintentional violation of privacy or security that may be caused by carelessness, lack of knowledge, lack of training, or other human error. Examples of this type of incident include directing PHI via mail, e-mail, or fax to a wrong party or incorrectly identifying a patient record.
- **Category 2: Failure to follow established privacy and security policies and procedures.** This is a violation due to poor job performance or lack of performance improvement. Examples of this type of incident include release of PHI without proper patient authorization; leaving detailed PHI on an answering machine; failure to report privacy and security violations; improper disposal of PHI; failure to properly sign off from or lock computer when leaving a work station; failure to properly safeguard password; failure to safeguard portable device from loss or theft; or transmission of PHI using an unsecured method.
- **Category 3: Deliberate or purposeful violation without harmful intent.** This is an intentional violation due to curiosity or desire to gain information, for personal use. Examples of this type of incident include accessing the information of high-profile people or celebrities or accessing or using PHI without a legitimate need to do so, such as checking the results of a coworker's pregnancy test.
- **Category 4: Willful and malicious violation with harmful intent.** This is an intentional violation causing patient or organizational harm. Examples of this type of incident include disclosing PHI to an unauthorized individual or entity for illegal purposes (i.e., identity theft); posting PHI to social media websites; or disclosing a celebrity's PHI to the media.

Sanctions may be modified based on mitigating factors. These factors may reflect greater damage caused by the violation and thus work against the violator, ultimately increasing the penalty.

Examples include:

- Violation of sensitive information such as HIV-related, psychiatric, substance abuse, and genetic data
- High volume of people or data affected
- High exposure for the organization
- Large organizational expense incurred, such as breach notifications
- Hampering the investigation, lack of truthfulness
- Negative influence on others
- History of performance issues and/or violations

Additional factors that could mitigate sanctioning include:

- Violator's knowledge of privacy and security practices (i.e., inadequate training, training barriers, or limited English proficiency)
- Culture of surrounding environment (i.e., investigation determines inappropriate practices in business unit)
- Violation occurred as a result of attempting to help a patient
- Victim(s) suffered no financial, reputational, or other personal harm
- Violator voluntarily admitted the violation in a timely manner and cooperated with the investigation
- Violator showed remorse
- Action was taken under pressure from an individual in a position of authority

Multifactor Model Categories

The multifactor sanctioning model identifies three categories of severity across four areas of risk. The organization takes corrective action and bases remediation on the highest level of category indicated. If a violation falls into one or more risk areas on the chart, the corrective action is based on the highest category level of risk.

Category	Exposure	Number Involved	Purpose	Special Protection
1	Low external exposure to organization	Involves a single patient	Ignorance or lack of education	No additional state or federal protections
2	Medium external exposure to organization	Involves 2–99 patients	Snooping or curiosity	Employees

3	High external exposure to organization	Involves 100+ patients	Malice, sale, or personal gain	HIV, mental health, adoption, etc.

Model 2—Multifactor Model

In this model the organization takes corrective action and bases remediation on the highest level of category indicated. This model contains four major areas of risk: organization exposure, number of patients involved, purpose of action causing violation, and involvement of PHI covered by "special protections" (e.g., HIV-related, psychiatric, substance abuse.) (See sidebar above for a breakdown of the different categories.)

If a violation falls into one or more risk areas, the corrective action is based on the highest category level of risk. For example, an error in the envelope-stuffing process for patient statements involving 1,000 patients would be a category 3 incident.

From incident to incident, appropriate investigation and managerial discretion is necessary in declaring that a violation occurred. Organizations may find a severity determination document useful for supporting the corrective action determination as well as for comparative purposes and oversight trending. A sample severity determination document is available [below].

Sanctions Policy Recommendations

Sanctions imposed for privacy and security violations must be consistent across the organization, regardless of the violator's status, with comparable discipline imposed for comparable violations. Organizational policy should address sanctions related to violations of both state and federal regulations as well as internal privacy and security policies. The policy should also address how the sanctions support the organization's human resource corrective action policy.

Organizations must establish general principles and processes that lead to fair and consistent outcomes, including the following:

1. The policy and procedures should be developed, documented, and approved by organizational leadership including legal, compliance, risk management, human resources, medical staff services, and others as applicable.
2. The policy should be written in a format that can accommodate ongoing updates to reflect modifications to the regulations, accreditation standards, and other organizational policies, including, but not limited to federal regulations (i.e., HIPAA, HITECH), state regulations (i.e., data breach notification laws, health codes), and accreditation standards (i.e., Joint Commission).
3. The policy should be aligned with other related organizational policies and contracts to ensure consistency across the organization, including, but not limited to, human resources policies and contracts, medical staff bylaws and rules and regulations, union contracts, vendor contracts, and business associate agreements.
4. The policy should be subject to defined oversight with defined reporting responsibility. A possible model would include an ad-hoc sanctions committee that reports to the privacy and security committee, which in turn reports to the compliance and oversight committee, and up to the audit and compliance committee of the board of trustees (see the figure "Sample Reporting Structure" on page 6).
5. The policy should be communicated and accessible to all workforce members (i.e., posted on the organization's intranet, available in policy manual, distributed to staff, and featured in workforce training).
6. The policy should address the appropriateness of applying the HITECH breach notification sanctions process if it is determined that unauthorized access, use, disclosure, or destruction has occurred.
7. The policy should address investigations of disclosures made by workforce members who are whistleblowers or victims of a crime as potential nonviolations. Examples of these types of disclosures include, but are not limited to, a workforce member acting on good faith who:

    - Believes that the organization has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or believes that the care, services, and conditions provided by the organization potentially endangers one (or more) patients, workforce members, or other members of the general public
    - Discloses PHI to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the organization
    - Discloses PHI to an appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the organization
    - Discloses PHI to an attorney retained by or on behalf of the workforce member for the purpose of determining legal options regarding disclosure conduct

The policy should address the organization's position on retaliatory action against a workforce member to ensure it does not intimidate, threaten, coerce, or discriminate against an individual who participates in the following activities:

- Files a complaint within the organization
- Files a complaint with the secretary of Health and Human Services
- Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing
- Opposes any act or practice unlawful under state and federal regulations, providing that the individual acted in good faith believing that the practice was unlawful, the manner of opposition was reasonable, and the individual's opposition did not involve disclosure of patient PHI in violation of regulations

The policy should address retention of pertinent sanctioning documentation according to state and federal requirements including organizational policy. (Note: the HIPAA privacy rule requires a minimum retention of six years.)

Defining Workforce Members, Terms, and Process

An organization's sanctions policy and enforcement provisions must be broad enough to encompass all workforce members who have access to PHI that is created and maintained by the organization. Workforce members, as defined by HIPAA, include employees, volunteers, trainees, and other persons whose conduct in the performance of work for a covered entity is under the direct control of such entity whether or not they are paid by the covered entity. This includes, but is not limited to:

- Medical staff members (employed and non-employed by the facility)
- Academic instructors
- Students
- Residents
- Board members
- Agency healthcare providers

Organizations must clearly define key terms in their sanctions policies, identifying violation categories and their respective sanctions (based on category). A clear sanction process will enable consistent enforcement across the organization. Consistent enforcement will prevent decisions from being overturned on appeal both internally and at administrative law hearings.

In addition, the sanction policy should:

- Clearly define leadership roles, including:
    - Role of the privacy or security officer to investigate and confirm the violation, including assignment of severity category
    - Role of human resources to determine appropriate sanction
    - Role of medical staff leadership for both employed and voluntary medical staff and other credentialed practitioners (i.e., nurse practitioners, nurse midwives, nurse anesthetists, and physician assistants) to determine appropriate sanction
    - Role of workforce member's manager to apply appropriate sanction
- Address what, if any, mitigating factors should be taken into consideration when determining the appropriate sanction (see list under "Model 1—Categories of Privacy and Security Incidents" for examples of mitigating factors)
- Support the human resources corrective action/disciplinary action policy and processes (if applicable)

Sample Reporting Structure

The graphic below illustrates a sample reporting structure for an organization's sanctions committee. Organizations should outline the sanctions committee's reporting structure in the sanctions policies and procedures.

Audit and Reporting Process

Organizations should create mechanisms and assign responsibilities for continuously monitoring sanctions to ensure consistent and equitable application across roles by violation category. Sanction data gathered for reporting purposes should include, but not be limited to, the following:

- Number of violations (by category) resulting in sanction
- Severity of sanction by category
- Severity of sanction by business unit and by role
- Trended data over time (e.g., monthly, quarterly, yearly)

The data should be reported to an interdisciplinary oversight committee to include at minimum the chief privacy official, chief security official, and senior personnel representing a broad array of departments such as compliance, labor, legal, IT, administration, medical staff, risk management, finance, and internal audit. The board of trustees or directors should also be included in the auditing and reporting process.

Organizations should evaluate the data they collect on disciplinary patterns to ensure comparable violations result in comparable sanctions for all roles within the organization and across all entities within a multi-site health system. The data should also be used to identify gaps and opportunities for improvement to the organization's privacy and security programs. In addition, the data can be communicated to the workforce as a deterrent and used to justify sanctions at grievances and other labor hearings.

Note

1. Ornstein, Charles. "Doctors Got off Lighter in UCLA Snooping Case." Los Angeles Times, April 12, 2008. http://articles.latimes.com/2008/apr/12/local/me-ucla12.

Appendix A: Sample Privacy and Security Violation Severity Determination Document

Fair and consistent patient privacy and security policy enforcement and sanction application across the PHI user base is critical to building trust in the organization, the industry, and the public. Each incident requires appropriate investigation along with managerial discretion to declare violation or breach.

A visual table like the one below can help to:

- Capture particular incident factors and sanction decisions
- Serve as a record or documentation
- Compare an incident to past incidents for consistency of approach and message
- Build trending statistics

This form and table can be used electronically or in paper copy for spreadsheet or database creation. Organizations can also use data elements from this form and table to create their own spreadsheet or database. This would serve as a confidential work document for assessment and improvement activities. It is intended for internal use only.

Individual Investigated: _____

Entity Name (if tracked): _____

Personnel Category: _____
(i.e., employed staff, contractual staff, volunteer, self-employed physician, business associate, etc.)

Date(s) of Incident(s): _____

Date of Discovery: _____

Method of Discovery: _____
(i.e., media, patient complaint, found on audit, internal staff report, etc.)

Description of Incident: _____
(Please attach additional documentation if needed)

Sanctions Applied (if applicable): _____

Date of Sanctioning: _____

Risk Analysis and Need for Breach Notification of Patients: _____

Comments: _____

Category Determination (highlight or circle all applicable) [Organizations can customize the category characteristics as desired]				
Category 1 Factors	Unintentional	Careless	Poor judgment	Lack of training/knowledge
Category 2 Factors	Deliberate	Unauthorized	No known redisclosure	Trained; understood policy
Category 3 Factors	Deliberate	Unauthorized	Redisclosure occurred	Trained; understood policy
Category 4 Factors	Deliberate	Unauthorized	Redisclosed for malice or personal gain	Understood policy

Sanction Impacting Factors (highlight or circle all applicable) [Organizations can customize the category characteristics as desired]								
Factors Increasing Sanction Severity	Multiple offenses	Harm incurred to victim(s)	Large number of victims	Large amount of data	High exposure to organi-zation	Hampered investigation	Large expense incurred (i.e., breach notification)	Actions influenced others
Factors Decreasing Sanction Severity	Occurred with good intentions (i.e., patient care, assist operations)	No harm to victim(s)	Volunteered /reported breach	Confessed/ cooperated with investigation	Showed remorse	Acted under direction of authority	Low cost to organization	

Sanctions Applied (highlight or circle all applicable) [Organizations can customize the category characteristics as desired]				
Lesser Sanction	Disciplinary process applied; Stage/Category #_____	Made example of (i.e., health system newsletter dept/company meeting)	Probation for ___ weeks / months	Suspended w/o pay ____ days/weeks
Stronger Sanction	Employment termination	Contract severance	Loss of medical staff privileges	

Instructions:

Forward original document to _____(list appropriate departments per policy)_____ Date submitted: _____

Report Completed by:

_____

**Discretion or adaptive use of this form may be necessary in circumstances of labor unions.*

References:

Section 13402(e)(4) of the HITECH Act

Prepared by:

Barb Beckett, RHIT, CHPS
Kathy Downing, MA, RHIA, CHP, PMP
Angie Fergen, RHIA, CHPS
Peg Schmidt, RHIA, CHPS

Acknowledgments

Ben Burton, JD, MBA, RHIA, CHP, CHC
Becky Buegel, RHIA, CHP, CHC
Kaye Connor, RHIT, CHC
Julie Dooling, RHIA
Elisa R. Gorton, RHIA, CPHS
Sandra L. Joe, MJ, RHIA
Lesley Kadlec MA RHIA
Joyce M. Matheson, RHIT
Kelly McLendon, RHIA
Kim Turtle Dudgeon, RHIT, HIT Pro-IS/TS, CMT
Diana Warner, MS, RHIA, CHPS, FAHIMA
Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Prepared by (Original)

Barbara Demster, MS, RHIA, CHCQM
Aviva Halpert, MA, RHIA, CHPS
Beth Hjort, RHIA, CHPS
Andrea Thomas-Lloyd, MBA, RHIA, CHPS

Acknowledgments (Original)

AHIMA 2008 Privacy and Security Practice Council
AHIMA 2009 Privacy and Security Practice Council

Article citation:
AHIMA. "Sanction Guidelines for Privacy and Security Violations (2013 update) - Retired" *Journal of AHIMA* 84, no.10 (October 2013): expanded web version.
