HIPAA Hints

New HIPAA Sanctions Policy Explained

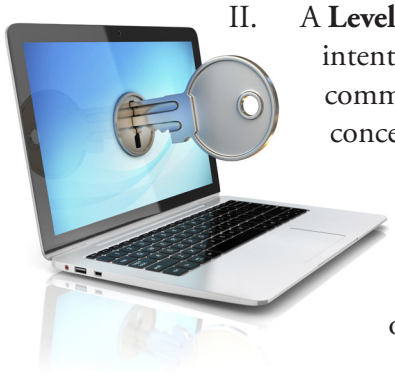
UAMS policies and procedures intended to protect the privacy and security of UAMS confidential information, including our patients' health information, are continuously adopted and reviewed and revised. These policies and procedures, such as the new HIPAA Sanctions Policy, are intended to ensure compliance with HIPAA so that UAMS fulfills its mission to improve the health, health care and well-being of Arkansans and of others in the region, nation, and the world.

The new HIPAA Sanctions Policy [**http://www.uams.edu/AdminGuide/PDFs/Section 2/2_1_42.pdf**] outlines procedures for disciplining UAMS employees for violations of HIPAA and UAMS HIPAA policies and procedures. The policy outlines three levels of HIPAA policy violations and disciplinary action for each level of violation.

The following are examples of the three levels of violations and a brief summary of potential disciplinary actions.

I. A **Level One** violation is unintentional or due to carelessness. Examples of a **Level One** violation are:
- inadvertently faxing, e-mailing or distributing protected health information (PHI) to the wrong person,
- discussing patient information in a public area, and
- failure to secure e-mail, text message or other electronic transmission of PHI.

A **Level One** violation will be grounds for progressive disciplinary action and will generally result in the employee receiving an oral warning.



II. A **Level Two** violation is intentional or purposeful or committed out of curiosity/ concern. Examples of a **Level Two** violation are:
- sharing a computer password with another individual(s) or using a password that belongs to someone else;
- intentionally or purposefully posting PHI on the internet (including, but not limited to, YouTube and social media sites such as Facebook, Instagram, Linked In, Twitter); and
- intentionally accessing any patient's record without a job-related reason.

A **Level Two** violation will be grounds for progressive disciplinary action and will generally result in the employee receiving a written warning.

III. A **Level Three** violation is for personal gain, acts of malice, or acts of gross misconduct. Examples of a **Level Three** violation are:
- inappropriately using or selling confidential information or PHI for personal or financial gain, such as accessing and using PHI in a court proceeding to receive personal or financial gain;
- falsifying or altering patient information; and
- deliberately compromising electronic information security measures.

Unless mitigating factors can be identified, **Level Three** violations will be treated as grounds for immediate dismissal under this policy.

The policy outlines the typical discipline with respect to each level of policy violation, and allows for circumstances that might result in a lower or higher level of discipline. Please refer to the policy for specific details and examples [**http://www.uams.edu/AdminGuide/PDFs/Section 2/2_1_42.pdf**].

The employee's manager and the HIPAA Privacy Officer and/or IT Security Officer will work with the Office of Human Resources to determine the appropriate level of the violation. The Office of Human Resources makes the final determination of any disciplinary action.

Please contact the HPAA Office at **(501) 603-1379** if you have questions or concerns regarding the policy.