KRIEG DEVAULT

Insights

Protected Health Care Communications Using Mobile Devices - How Does Your Policy Rate?

April 5, 2017

By: Susan E. Ziel

Do you have a corporate policy that governs your "protected communications" which may be sent or received through the use of mobile devices? If yes, does your Policy address each of the following "Top 10" requirements? Here's a checklist to assist you in reviewing, updating (and communicating) your Policy, today!

1.) Key Terms. The Policy shall define certain key terms, including, but not limited to, Applicable :Requirements (i.e., Federal and State laws governing the privacy and security of protected health and other personal information), Protected Health (and Other Personal) Information (PHI), Protected Communications (i.e., e-mails or texts containing PHI) and Mobile Devices (i.e., laptop, tablet, smart phone).

2.) Policy Prohibition. The Policy shall begin with an affirmative prohibition that absolutely no personnel are permitted to use any Mobile Device, regardless of ownership, to send or receive any Protected Communication, whether on or off premises, on or off duty, except in accordance with all requirements set out in the Policy. The Policy should also state an absolute prohibition of any social media communications or posts that contain PHI.

3.) Authorized Mobile Devices. The Policy shall state all administrative, physical and technical safeguards necessary for a designated representative (i.e., Security Officer) to authorize a particular Mobile Device, whether owned by the organization or the individual, for use under the Policy. The Policy should also include (or cross-reference to) an up-to-date log of all Authorized Mobile Devices.

4.) Authorized Software and Applications (Apps). The Policy shall state all administrative, physical and technical safeguards necessary for a designated representative (i.e. Security Officer) to authorize particular Mobile Device software and applications for use under the Policy.

5.) Authorized Users. The Policy shall state the requirements necessary for a designated representative (i.e., Chief Executive Officer) to authorize a particular individual, or alternatively, a particular job category, to use Authorized Mobile Devices under the Policy. The Policy should also include (or cross-reference to) an up-to-date list of all Authorized Users, either by name or job category.

6.) Authorized (and Necessary) Purposes. The Policy shall specify the particular circumstances when Authorized Users may use Authorized Mobile Devices to send or receive Protected Communications for authorized (and necessary) purposes.

7.) Additional Safeguards. The Policy shall specify any additional safeguards that are necessary to limit the risk of any unauthorized access to a Mobile Device that continues to store a Protected Communication after the communication has been completed.

8.) Missing Mobile Devices. The Policy shall require all personnel to immediately report any missing Mobile Device that may store a Protected Communication to a designated representative (i,e,, Security Officer) so to permit a prompt investigation and to mitigate and correct any losses or violations resulting from the incident.

9.) Sanctions. The Policy shall state all internal and external sanctions that may result from an individual's violation of this Policy, including but not limited to the civil and criminal penalties arising under Applicable Requirements.

10.) Frequently Asked Questions. The Policy should also attach a series of "frequently asked questions" that are answered concisely with examples, as much as possible.

If we can assist your organization in updating your Protected Health (and Other Personal) Information Privacy and Security Policies and related forms, please contact us at Integrity Health Strategies for additional information about our cost-effective, fixed-fee service arrangements.