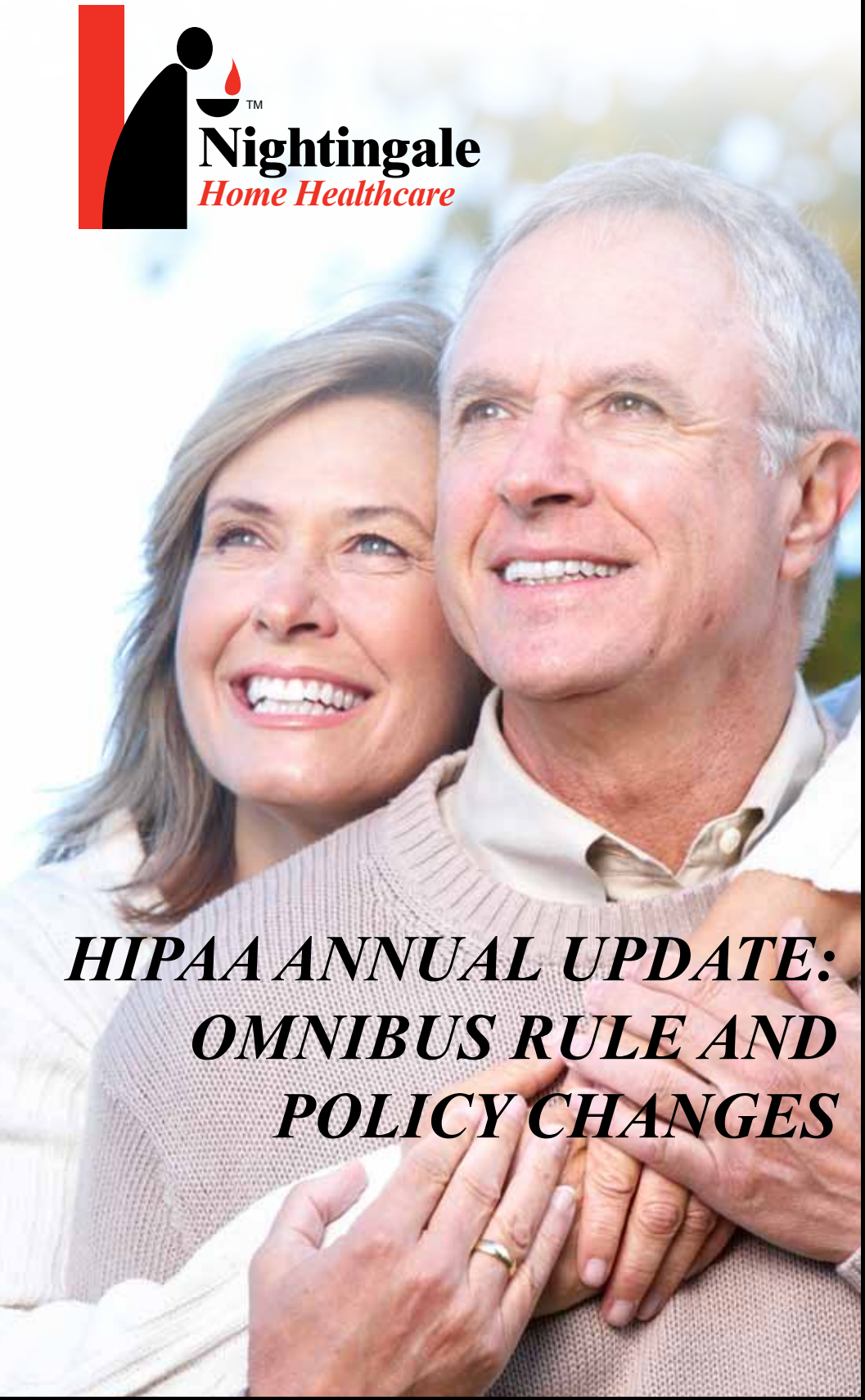
Nightingale™
Home Healthcare



HIPAA ANNUAL UPDATE: OMNIBUS RULE AND POLICY CHANGES

Nightingale™
Home Healthcare

Here's what you need to know:

The U.S. Department of Health and Human Services strengthened protections for health information established under the HIPAA of 1996. The final omnibus rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law.

New Requirements for Business Associates:

Previously, HIPAA regulations covered any business associate or contractor whose work involved the use or disclosure of individually identifiable health information, such as a contracted therapist who provided therapy services to our patients. Under the latest regulations, business associate status is triggered when a person or company "creates, receives, maintains or transmits" personal health information. The key addition in this part of the regulation is 'maintains'. Any company that 'maintains' protected health information on behalf of our agency - even if no access to that information is required or expected - will now be a business associate.

Under the Final Rule, business associates and their subcontractors are directly liable for the following Privacy requirements, even if they never entered into a business associate agreement:

- Impermissible uses and disclosures of protected health information;
- Failure to enter into a business associate agreements with subcontractors;
- Failure to provide breach notification to our agency;
- Failure to provide access to a copy of electronic protected health information to either the covered entity or the owner of the data and;
- Failure to disclose protected health information when required by the US. Department of Human and Health Services; and failure to provide an accounting of disclosures of protected health information upon request.

Under the new rule, penalties are increased for noncompliance based on the level of

Nightingale
Home Healthcare

negligence with a maximum penalty of $1.5 million per violation.

Protected Health Information Breach

Under the previous rules, an impermissible use or disclosure of protected health information - including electronic - was a breach if it posed a risk of harm to the individual. The U.S Department of Human and Health Services included in the new rules a presumption that any impermissible use or disclosure of protected health information is a breach, subject to breach notification rules. The only way to get out of this presumption is by a demonstration that there is a low probability that the protected health information was compromised. To demonstrate low probability, our agency must perform a risk assessment of four factors at a minimum:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the protected health information or to whom the disclosure was made.
3. Whether the protected health information was actually acquired or viewed.
4. The extent to which the risk to protected health information has been mitigated.

The US Department of Human and Services has indicated that it expects these risk assessments to be thorough and completed in good faith and to reach reasonable conclusions. If the risk assessment does not find a low probability that protected health information has been compromised, then breach notification is required.

Here are some more important parts of the HIPAA Omnibus Rule:

- Extends the requirements of the privacy and security rules business associates and their subcontractors
- Establishes new limitations on the use of protected health information for marketing and fundraising purposes

Nightingale
Home Healthcare

- Prohibits the sale of a patient's protected health information without specific individual authorization to do so
- Expands patients' rights to request and receive electronic copies of their protected health information
- Broadens patients' ability to restrict, in some instances, disclosure of their protected health information to health insurance plans
- The rule also requires companies to update their individual notice of privacy practices

Here's what you need to do now:

The US Department of Human and Health Services have stepped up scrutiny to make sure businesses are following the Omnibus Rule. Our agency has revised our Business Associate Agreements, Notice of Privacy Practices, breach and risk assessments, policies, and training as described above for those who have access to the protected health information of our employees and patients.

» Use the updated Business Associate Agreement (BAA). It has been distributed to all locations along with instructions to review and update contractor BAA as needed.
» Provide the updated Notice of Privacy Practices to patients. It is part of the Patient Orientation Booklet and is posted on our website at http://homecareforyou.com/.
» Complete this training update and the associated quiz.
» Report. If a violation of a privacy policy or procedure is suspected or detected, you must report it immediately. To complete & submit an online report, visit http://homecareforyou.com/. Click to enter the Intranet website. Log in, select the report form OR contact your manager.