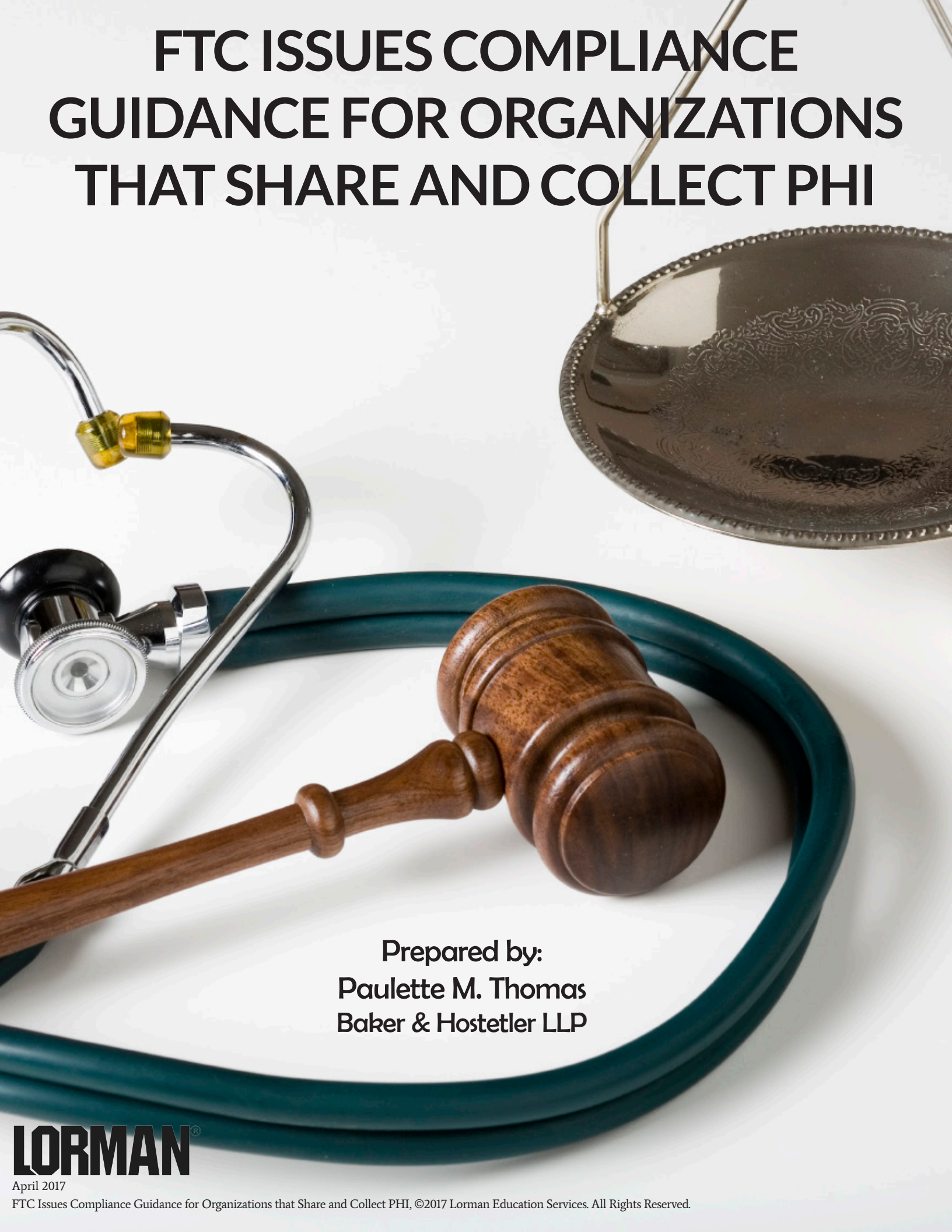


FTC ISSUES COMPLIANCE GUIDANCE FOR ORGANIZATIONS THAT SHARE AND COLLECT PHI



Prepared by:
Paulette M. Thomas
Baker & Hostetler LLP

LORMAN®

April 2017
FTC Issues Compliance Guidance for Organizations that Share and Collect PHI, ©2017 Lorman Education Services. All Rights Reserved.

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you **UNLIMITED** access to Lorman's ever-growing library of training resources:

- ✓ Unlimited Live Webinars - 120 live webinars added every month
- ✓ Unlimited OnDemand and MP3 Downloads - Over 1,500 courses available
- ✓ Videos - More than 700 available
- ✓ Slide Decks - More than 1700 available
- ✓ White Papers
- ✓ Reports
- ✓ Articles
- ✓ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.



Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

FTC Issues Compliance Guidance for Organizations that Share and Collect PHI

By Paulette M. Thomas

The Federal Trade Commission (FTC) recently issued Guidance to remind HIPAA compliant organizations that share and collect protected health information (PHI) for commercial activities that they must also comply with FTC Act disclosure requirements. The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. The Guidance cautions that organizations should consider all disclosure statements made to consumers to ensure that when taken together, they don't create a deceptive or misleading impression.

HIPAA Compliance

HIPAA regulations require that covered entities and business associates obtain an authorization to use and disclose an individual's PHI for "commercial activities besides treatment, payment, health care operations, or other uses and disclosures permitted or required by the Privacy Rule." As a result, "the consumer must first give you written permission through a valid HIPAA authorization," according to the Guidance. The authorization must be in plain language so the individual can understand it and include specific terms and a description of how the individual's information will be used.

FTC Act Compliance

The FTC cautions that while an organization's authorization and disclosure practices may be compliant with HIPAA, they must also comply with the FTC Act. Section 5(a) of the FTC Act, codified at 15 U.S.C. § 45(a), prohibits unfair or deceptive acts or practices in or affecting commerce and applies to all persons engaged in commerce. Under the FTC Act, the legal standard for unfairness and deception are independent of each other. An act or practice may be found to be unfair where it causes, or is likely to cause, substantial injury to consumers that is not reasonably avoidable by the consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

In order to determine whether a representation, omission, or practice is deceptive, the FTC uses a three-part test:

1. The representation, omission, or practice misleads or is likely to mislead the consumer;
2. The consumer's interpretation of the representation, omission, or practice must be reasonable under the circumstances; and
3. The misleading representation, omission, or practice must be material.
4. *Action Items for Evaluating Organizational Compliance*

Organizations should evaluate their promotional practices and requests to use an individual's PHI for marketing or commercial purposes. To that end, the Guidance sets out the following considerations for assessing organizational compliance and strategies to avoid or reduce noncompliance risks:

- Review user interface, privacy policy, terms of use, and notice of privacy practices for consistency of statements, and evaluate whether the information would be considered deceptive.
- Evaluate the communication's content for promises or assurances made to protect the privacy and security of the information, and determine if these are reasonable compared to the practices in place.
- Review and evaluate the website content and navigational processes, and review for fine print or inconspicuous disclosures that may be relevant to headlines or conspicuous postings.
- Be aware of targeted or vulnerable audiences such as the elderly when preparing communications.
- Review alternative forms of communication such as texting or using mobile apps, and paper documents.
- Coordinate with the organization's marketing department and other stakeholders to implement a process to review communications prior to implementation or posting to the website.

