

Reproduced with permission from Privacy & Security Law Report, 13 PVLR 1756, 10/13/2014. Copyright © 2014 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## 'Health Care'-Related Calls: Ambiguity at the Intersection of HIPAA and TCPA



BY MARC S. ROTH, HELEN R. PFISTER AND ANNE O'HAGAN KARL

The Federal Communications Commission (FCC) has established exemptions from certain requirements of the Telephone Consumer Protection Act (TCPA) for health care messages regulated under the Health Insurance Portability and Accountability Act (HIPAA).<sup>1</sup> Although this exemption initially appears to give health care providers broad latitude in calling or texting patients, there is ambiguity as to the scope of the exemption. Specifically, the TCPA exemption applies to "health care" messages regulated under HIPAA, but HIPAA does not expressly define "health care" messages. The different uses of terminology may create confusion for providers and health insurers.

### TCPA and the 'Health Care' Messages Exemption

In general, the TCPA prohibits entities from making certain types of calls to consumers without their con-

sent. Specifically, the TCPA prohibits calls and text messages (collectively referred to as "calls")<sup>2</sup> transmitted to a consumer's mobile device using an autodialer, as well as prerecorded messages placed to a landline, without the recipient's prior consent. In enacting the TCPA, Congress intended to protect consumers' privacy in their home and on their mobile phone by banning autodialed and prerecorded marketing calls and to provide them with the ability to control from whom they receive such calls.<sup>3</sup>

Under the FCC rules implementing the TCPA (TCPA Rules),<sup>4</sup> the type of consent that an entity must obtain from the consumer differs depending on whether the call contains a commercial message.<sup>5</sup> If a call contains a noncommercial message, the TCPA Rules require only the consumer's "express consent" to receive such calls. The FCC has stated that express consent may be obtained when the consumer provides her or his mobile phone number to the caller.<sup>6</sup> On the other hand, for

<sup>1</sup> Pub. L. No. 104-191 (1996).

*Marc S. Roth is a partner in the Advertising, Marketing & Media Practice Group at Manatt, Phelps & Phillips LLP in New York and co-chair of the firm's TCPA Compliance and Class Action Defense Group.*

*Helen R. Pfister is a partner in Manatt's Healthcare Practice Group in New York.*

*Anne O'Hagan Karl, an associate in Manatt's Healthcare Practice Group in New York, assisted in the preparation of this article.*

<sup>2</sup> A text message is considered a telephone call under the TCPA. *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CC Docket No. 92-90, Report and Order, 7 FCC Rcd 8752, 8774, ¶ 43 (1992) (concluding that text messages would be subject to the TCPA); *Satterfield v. Simon & Schuster Inc.*, 569 F.3d 946 (9th Cir. 2009) (8 PVLR 959, 6/29/09).

<sup>3</sup> TCPA, Pub. L. No. 102-243.

<sup>4</sup> 47 C.F.R. §§ 64.1200, et seq.

<sup>5</sup> For purposes of this article, "commercial" shall mean "advertisements" and "telemarketing," as those terms are defined in the TCPA Rules, C.F.R. §§ 64.1200(f)(1), 64.1200(f)(12) (2012).

<sup>6</sup> The TCPA and the TCPA Rules do not define "express consent," but the FCC and most courts have held that the provision of a mobile number by a consumer to the calling/texting party satisfies this requirement. *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*,

commercial calls, the TCPA Rules require that the recipient provide her or his “*express written consent*,” a higher standard that was established in new rules promulgated by the FCC that went into effect Oct. 16, 2013 (the 2013 Rule Change).<sup>7</sup> This standard must be met in order to transmit advertisements and telemarketing messages to consumers’ mobile devices and place pre-recorded calls to consumers’ landline phones.<sup>8</sup> Unlike the lesser *express consent* standard for noncommercial calls, the new, higher standard has specific disclosure requirements, as detailed in the 2013 Rule Change.<sup>9</sup>

Accordingly, absent a specific regulatory exemption, health care providers that either call or transmit text messages to patients’ mobile phones using an autodialer or make pre-recorded calls to landlines would generally need to obtain prior consent from patients—express consent if the call or text message contains a noncommercial message, and express written consent if the call contains a commercial message. Also note that if a message is intended to be noncommercial but contains any commercial messaging, it would be considered a “dual-purpose” call, thus triggering the more stringent express written consent standard.<sup>10</sup>

### The ‘Health Care’ Message Exemption

Pursuant to the TCPA, the FCC is authorized to establish exemptions from the law’s consent requirements for (1) noncommercial calls and (2) commercial calls that do not adversely affect the privacy rights of the called party or where a consumer’s privacy is otherwise protected by law.<sup>11</sup>

In the 2013 Rule Change, the FCC created an exemption from the *express written consent* requirement for calls that contain a commercial “health care” message made by, or on behalf of, a “covered entity” or its “business associate,” as those terms are defined in the HIPAA Privacy Rules.<sup>12</sup> Therefore, the TCPA Rules expressly exempt from the *express written consent* requirements commercial calls made to a consumer’s mobile device and pre-recorded messages to landlines that

contain a “health care” message under the HIPAA Privacy Rules.

When creating this exemption, the FCC expressly adopted the reasoning previously set out by the Federal Trade Commission (FTC) in its modification of the Telemarketing Sales Rule (TSR) in 2008.<sup>13</sup> The FCC concurred with the FTC’s reasoning for exempting health care-related messages from the TSR.<sup>14</sup> Specifically, the FCC noted that in establishing the exemption for health care-related messages the FTC listed the following six reasons:

- the delivery of health care-related pre-recorded calls subject to HIPAA is extensively regulated by the federal government;

- subjecting health care-related calls to the TSR could create inconsistencies with HIPAA and other federal statutes governing health care programs, frustrating congressional intent;

- the number of health care providers that might call a patient is limited, in “sharp contrast to the virtually limitless number of businesses” that could make calls to consumers;

- there is no incentive for providers that make health care-related pre-recorded calls to attempt to increase sales “through an ever-increasing frequency or volume of calls”;

- the “reasonable consumer” would likely not view pre-recorded health care calls as coercive or abusive; and

- health care-related calls have not been the focus of the type of privacy abuses that the TSR was intended to remedy.<sup>15</sup>

Interestingly, the FCC did not exempt noncommercial calls conveying health-related messages made to a consumer’s mobile device and noncommercial pre-recorded messages to landlines. As such, to place such calls, the caller need only obtain the called party’s *express consent*. Under the TCPA Rules, as noted above, the calling party obtains an individual’s express consent when the individual provides her or his phone number with the reasonable expectation that the number will be used to communicate with her or him in connection with the purpose for which it was provided.<sup>16</sup> Therefore, as long as a caller obtains a consumer’s mobile number from the consumer, uses it in connection with the purpose for which it was provided and the intended call does not contain a commercial message, the caller does not need to obtain any additional consent.

In sum, entities sending “health care” messages regulated under HIPAA do not need to obtain express written consent prior to calling a consumer’s mobile phone using an autodialer or transmitting pre-recorded messages to a landline, but must still obtain “express consent.”

### HIPAA Regulation of Health Information

In establishing the exemption for “health care” messages, the FCC referred to the extensive regulation of

CC Docket No. 92-90, Report and Order, 23 FCC Rcd 559, 564 (2008) (the 2008 FCC Ruling); *Mais v. Gulf Coast Collection Bureau, Inc.*, No. 13-14008, 2014 BL 274279 (11th Cir. Sept. 29, 2014) (13 PVL 1731, 10/6/14). However, some courts have qualified this approach by considering the manner and context by which a consumer provides her number, and the consumer’s understanding and expectation of how her number will be used. See *Kolinek v. Walgreen Co.*, No. 1:13-cv-04806, 2014 BL 232925 (N.D. Ill. Aug. 11, 2014) (12 PVL 1067, 6/17/13).

<sup>7</sup> 2013 Rule Change, ¶¶ 32-34 (2012) (11 PVL 924, 6/11/12); 47 C.F.R. §§ 64.1200(a)(2), 64.1200(f)(8) (2012).

<sup>8</sup> 47 C.F.R. § 64.1200(f)(8). *In re Rules and Regulations Implementing the TCPA*, 27 FCC Rcd. 1830, 1838, ¶¶ 20-26 (Feb. 15, 2012). Although the FCC promulgated these rules in 2012, they did not become effective until 2013 (11 PVL 1581, 10/29/12).

<sup>9</sup> *Id.*

<sup>10</sup> See *Chesbro v. Best Buy Stores LP*, 697 F.3d 1230 (9th Cir. 2012) (citing FCC discussion of “dual-purpose” calls in 2003 Report and Order, at 14097-98, ¶¶ 140-142). The U.S. Court of Appeals for the Ninth Circuit upheld a district court finding that pre-recorded “courtesy” messages made by Best Buy to its Best Buy Reward Zone members regarding unused program certificates were not solely “informational,” but rather, dual-purpose telemarketing calls, as they encouraged consumers to make a purchase (11 PVL 1557, 10/22/12).

<sup>11</sup> 47 U.S.C. § 227(b)(2)(B).

<sup>12</sup> 45 C.F.R. § 160.103; 47 C.F.R. § 64.1200(a)(2) and § 64.1200(a)(3)(v) (2012).

<sup>13</sup> See 16 C.F.R. § 310; see also 73 Fed. Reg. 51,164 (Aug. 29, 2008).

<sup>14</sup> 77 Fed. Reg. 34,233, 34,240 (June 11, 2012).

<sup>15</sup> *Id.*

<sup>16</sup> See *supra* note 6.

such messages under HIPAA. However, although HIPAA extensively regulates many uses and disclosures of certain types of health-related information by health insurers and most health care providers, HIPAA does not expressly define “health care” messages, creating ambiguity with respect to the “health care” messages exemption under the TCPA.

The HIPAA Privacy and Security Rules<sup>17</sup> regulate how health insurers and most health care providers, such as hospitals and physicians (collectively referred to as covered entities), use or disclose health care information. If a covered entity elects to use a vendor to perform certain tasks on its behalf, the vendor is referred to as a “business associate,” and the business associate is also subject to most requirements under the HIPAA Privacy and Security Rules.<sup>18</sup>

HIPAA’s requirements do not apply to all types of health care information. Instead, HIPAA applies primarily to “protected health information” (PHI), which is defined as individually identifiable information that:

- (1) is created or received by a health care provider . . . and
- (2) relates to the past, present, or future physical or mental health or condition of that individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.<sup>19</sup>

#### **HIPAA Privacy Rule Governs the Purposes for Which Covered Entities May Use or Disclose PHI**

The HIPAA Privacy Rule governs how covered entities and their business associates may use or disclose PHI. Covered entities and business associates may not use or disclose PHI unless either (1) the HIPAA Privacy Rule expressly permits or requires a specific use or disclosure or (2) the individual whose information would be used or disclosed (or the individual’s representative) authorizes the use or disclosure in writing.<sup>20</sup>

HIPAA permits covered entities and business associates to use or disclose PHI without a patient’s authorization for, among other things, treatment, payment or health care operations.<sup>21</sup> For example, a physician could submit information about a patient’s treatment to a health insurer in order to receive payment without first obtaining the patient’s authorization.

The HIPAA Privacy Rule, however, requires that individuals provide written authorization before a covered entity (or business associate) may use their PHI for “marketing” purposes.<sup>22</sup> “Marketing” does **not** include the use or disclosure of PHI (i) for treatment by a health care provider; (ii) to describe a health-related product or service that is provided by the covered entity (or, for health insurers, included in a plan’s benefit package) making the communication; or (iii) for case management, care coordination, contacting individuals about treatment alternatives or related activities that do not constitute treatment.<sup>23</sup> These exceptions to the definition of “marketing” do not apply if the covered entity receives payment for making the communications from the party whose products or services are being promoted. In other words, if an MRI manufacturer pays a

hospital to call patients and inform them about the hospital’s new MRI service, that communication would constitute “marketing” under HIPAA. Third parties may, however, pay covered entities to transmit refill reminders, including information about the patient’s current medication or a generic substitute, without the communication constituting “marketing,” so long as the payment reasonably relates to the cost of the communication.<sup>24</sup>

Covered entities or their business associates using or disclosing PHI when contacting a patient must first assess the purpose for contacting the patient. If the covered entity is contacting the patient for a marketing purpose, then HIPAA requires that the covered entity first obtain the individual’s written authorization. By contrast, if the covered entity is contacting the patient for a purpose permitted under the Privacy Rule, such as to convey information about the patient’s ongoing treatment, a written authorization is not needed.

#### **HIPAA Security Rule Regulates the Mechanisms Covered Entities Use to Share PHI**

Regardless of whether the TCPA exemption applies, all communications containing or concerning PHI must comply with the HIPAA Security Rule. Under the HIPAA Security Rule, messages sent by covered entities (or a business associate on their behalf) that contain PHI must be sent securely.<sup>25</sup> Such messages must be sent in a way that guards against unauthorized access, and covered entities (or business associates acting on their behalf) must “address” whether or not to use encryption.<sup>26</sup> Under the HIPAA Security Rule, entities are required to assess whether it is “reasonable and appropriate” to deploy encryption—and if not, they must document why it would not be reasonable and appropriate and implement an equivalent alternative measure.<sup>27</sup>

Although covered entities and their business associates must comply with the HIPAA Security Rule in their electronic communications with patients, regulators have clarified that a patient has the right to receive communications from their health care providers in the form or format that works best for the patient—even if the method preferred by the patient for receiving health care messages is insecure. For example, the Department of Health and Human Services Office for Civil Rights, which enforces the HIPAA Privacy and Security Rules, recently clarified that HIPAA-covered entities are permitted to send an individual unencrypted e-mail if they have provided the individual with a “light warning” advising the individual that the e-mail will be unsecure and the patient nevertheless prefers to receive information by unencrypted e-mail.<sup>28</sup> Specifically, on the issue of what constitutes a “light warning,” HHS noted the following:

We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the e-mail could be read by a third party. If the individuals are notified of the risks and still prefer unencrypted e-mail, the individual has the right to receive [PHI]

<sup>17</sup> 45 C.F.R. §§ 160, 164.

<sup>18</sup> 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e).

<sup>19</sup> 45 C.F.R. § 160.103.

<sup>20</sup> 45 C.F.R. § 164.502(a).

<sup>21</sup> 45 C.F.R. § 164.506(c).

<sup>22</sup> 45 C.F.R. §§ 164.501, 164.508(a)(3).

<sup>23</sup> 45 C.F.R. § 164.501.

<sup>24</sup> *Id.*

<sup>25</sup> See HIPAA Security Rule for additional details on what constitutes a secure message.

<sup>26</sup> 45 C.F.R. § 164.314(e)(1)(2)(ii).

<sup>27</sup> 45 C.F.R. § 164.306(d)(3).

<sup>28</sup> 78 Fed. Reg. 5566, 5634 (2013).

in that way, and covered entities are not responsible for unauthorized access of [PHI] while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual.<sup>29</sup>

## Putting HIPAA and the TCPA Together

As is discussed above, the TCPA exempts "health care" messages made by covered entities or their business associates from the requirement to obtain an individual's express written consent under the TCPA to make certain types of phone calls. HIPAA, however, addresses the use and disclosure of PHI, not all "health care" information. Further, HIPAA does not expressly address or define "health care" messages. For health care providers intending to contact individuals on their mobile phones using an autodialer or to transmit prerecorded messages to a landline, this disconnect between the terminology used in the TCPA and HIPAA creates compliance challenges.

Litigation and guidance from the FCC may begin to answer some of the questions over how to interpret the scope of the TCPA's exemption for "health care" messages. Several cases in 2013 and 2014 address automated messages in the health care context. In one case, *Kolinek v. Walgreen Co.*, the plaintiff alleges a violation of the TCPA for automated refill reminder calls from Walgreens pharmacies.<sup>30</sup> In a 2013 case, the plaintiff objected to automated calls from a collections agency working on behalf of a radiologist in connection with an unpaid bill for services rendered to the plaintiff during an emergency room visit, and the district court granted summary judgment on the plaintiff's behalf.<sup>31</sup>

Although both of these cases involved health-related matters, neither, unfortunately, addressed head-on the issue of whether the messages were "health care"-related and thus exempt under the TCPA. Instead, they both turned on whether the plaintiff granted express consent to be contacted. Specifically, whether the fact that the patient provided her phone number for one purpose constituted "express consent" for other uses of the number. Even though neither case addresses the

scope of the "health care" messages exemption, it suggests that consumers are noticing automated calls from or on behalf of health care providers and intend to assert their rights under the TCPA.

Until courts or the FCC are called upon to clarify some of the ambiguity surrounding these issues, covered entities and business associates should consider the following questions before making automated calls to patients' mobile devices or prerecorded calls to their landlines:

- *Is it PHI?* If the information being transmitted contains or concerns PHI, then the covered entity must ensure that the communication complies with HIPAA.

- *If it is PHI, is it marketing?* The covered entity must assess whether or not the call would constitute marketing under the HIPAA Privacy Rule. If it does constitute "marketing," then the covered entity must first obtain the patient's written authorization.

- *If it is PHI but not marketing, is the call for "commercial" purposes?* If the covered entity is using or disclosing PHI but the call is not marketing, the covered entity should next consider whether the call is for "commercial" purposes. As is discussed above, the "health care" messages exemption applies only to "commercial" automated calls. Noncommercial automated calls delivering "health care" messages still require the patient's express consent. Although the provision of a phone number by a patient may constitute "express consent" under the TCPA, recent court cases have raised questions about whether the patient must specifically agree to receive certain types of calls from providers.

- *If it is not PHI, is it a "health care" message?* If the covered entity is not using PHI, then the covered entity must consider whether the message would constitute a "health care" message. Without a definition of "health care" message under HIPAA, there is no clear line between "health care" messages and other types of messages from covered entities. Accordingly, the covered entity must assess each call on a case-by-case basis. For example, a call by a national pharmacy chain advertising their photo-printing service would not constitute a "health care" message, and thus express written consent would be required before the covered entity made automated calls. By contrast, a call from the same pharmacy chain providing information on the availability of influenza vaccinations arguably would constitute a "health care" message, and thus express written consent would not be required.

<sup>29</sup> *Id.*

<sup>30</sup> *Kolinek v. Walgreen Co.*, No. 1:13-cv-04806, 2014 BL 232925 (N.D. Ill. Aug. 11, 2014).

<sup>31</sup> *Mais v. Gulf Coast Collection Bureau Inc.*, 944 F. Supp. 2d 1226 (S.D. Fla. 2013). However, the district court's summary judgment decision was subsequently overturned by the U.S. Court of Appeals for the Eleventh Circuit, finding that the district court lacked the power to consider the validity of the 2008 FCC Ruling. *See supra* note 6.

**NEW PORTFOLIOS  
& TREATISES  
NOW AVAILABLE**

# SAFE DATA & SOUND SOLUTIONS



## Privacy & Data Security Law Resource Center™

Unparalleled news. Expert analysis from the new Privacy & Data Security Portfolio Practice Series. Comprehensive new treatises. Proprietary practice tools. State, federal, and international primary sources. The all-in-one research solution that today's professionals trust to navigate and stay in compliance with the maze of evolving privacy and data security laws.

**TO START YOUR FREE TRIAL  
CALL 800.372.1033 OR  
GO TO [www.bna.com/privacy-insights](http://www.bna.com/privacy-insights)**

# Bloomberg BNA