

KATIE PORTER
45TH DISTRICT, CALIFORNIA

FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON
INVESTOR PROTECTION, ENTREPRENEURSHIP, AND
CAPITAL MARKETS
SUBCOMMITTEE ON
CONSUMER PROTECTION AND FINANCIAL SERVICES

Congress of the United States
House of Representatives
Washington, DC 20515-0545

WASHINGTON OFFICE:
1117 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-5611

DISTRICT OFFICE:
2151 MICHELSON DRIVE
SUITE #195
IRVINE, CA 92612
(949) 668-6600
porter.house.gov

February 28, 2020

Kathy Kraninger
Director
Consumer Financial Protection Bureau
1700 G St NW
Washington, D.C. 20552

Alex Azar
Secretary
Department of Health and Human Services
200 Independence Avenue SW
Washington, D.C. 20201

Dear Director Kraninger and Secretary Azar,

I write to you today to raise concerns over medical debt collection practices that are jeopardizing the privacy and financial security of patients across the country. Specifically, I am deeply concerned that some elements of the Consumer Financial Protection Bureau's (CFPB) proposed rule to implement the Fair Debt Collection Practices Act may place patients' protected health information at risk.¹ Before this proposed rule reaches its final stages, I request that the CFPB collaborate with the Department of Health and Human Services (HHS) to conduct—and make public—a formal review of the privacy, health, and financial implications of this proposed regulation and incorporate the results into any rulemaking.

According to the CFPB's own research, as of 2014, more than 43 million Americans had medical debt that negatively affected their credit reports. Moreover, half of all overdue debt on credit reports came from medical bills.² Since the CFPB completed this research in 2014, the number of Americans facing insurmountable healthcare costs and growing medical debt has continued to increase. A recent academic study found that approximately two-thirds of all bankruptcies were tied to medical issues.³ Additional research has found that nearly 137.1 million Americans "faced financial hardship" because of medical costs.⁴

The stated intent of the CFPB's proposed rule is to protect consumers from predatory debt collection practices and to update existing law to address the use of electronic communications in debt collection.⁵ However, the proposed rule fails to protect patients and their private health information from a pernicious new trend in medical debt collection: the use of social media platforms and texting to contact consumers.⁶

The CFPB's May 2019 proposal only prohibits debt collectors from using "a social media platform that is viewable by a person other than the consumer."⁷ This leaves a glaring loophole

¹ <https://www.consumerfinance.gov/about-us/newsroom/bureau-proposes-regulations-implement-fair-debt-collection-practices-act/>

² <https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-medical-debt-collector/>

³ <https://www.cnbc.com/2019/02/11/this-is-the-real-reason-most-americans-file-for-bankruptcy.html>

⁴ <https://link.springer.com/article/10.1007/s11606-019-05002-w>

⁵ <https://www.consumerfinance.gov/about-us/newsroom/bureau-proposes-regulations-implement-fair-debt-collection-practices-act/>

⁶ <https://www.consumerfinance.gov/about-us/newsroom/bureau-proposes-regulations-implement-fair-debt-collection-practices-act/>

⁷ https://files.consumerfinance.gov/f/documents/cfpb_debt-collection-NPRM.pdf

in the use of social media and text messaging to communicate directly with consumers, defined as “any act to initiate a communication or other contact with any person through any medium, including by soliciting a response from such person.”⁸ Despite many potential privacy vulnerabilities, this likely includes a Facebook “friend request” or LinkedIn “connection”—practices that recent reports suggest are already in use.⁹

On March 8, 2011, Joclyn Krevat, a patient who had recently been admitted to the hospital and diagnosed with giant cell myocarditis, an inflammatory heart disease that can cause heart failure, received a request on LinkedIn from a debt collector.¹⁰ At the time, Krevat was carrying an estimated \$50,000 in medical debt.¹¹ While this communication may be compliant with the proposed rule, it likely constitutes a violation of longstanding health privacy laws overseen by HHS and the Federal Trade Commission (FTC).¹²

Sharing a patient’s protected health information, including for the purposes of debt collection, must comply with the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Privacy Rule established national standards to protect patients’ medical records and other personal health information.¹³ The Privacy Rule applies to “covered entities:” health plans, health care clearinghouses, and certain health care providers—as well as “business associates:” outside organizations that manage services for the covered entity, such as billing.¹⁴

HIPAA does contain a limited exemption for debt collection, (referred to as Section 1179), but when Congress enacted this provision in 1996 it was not contemplated that debt collection would occur in public settings.¹⁵ Based on HHS’ own Report to Congress called “Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA,” there is no doubt that social media is public.¹⁶ It is well established that anything posted on social media is not only exposed to anyone in the person’s social network; the data in such posts also becomes the property of, and is used without significant privacy protections, by the social media platform. By permitting communications about medical debt collection to occur on social media as CFBP proposes, these rules run the serious risk of exacerbating an already concerning privacy environment.

By contrast to the limited scope of financial industry practices contemplated by Section 1179, a congressionally-mandated HHS report to Congress outlined the public nature of social media and its troubling implications for the privacy and security of health data.¹⁷ But for Section 1179, a medical debt collection agency working on behalf of a covered entity like a hospital or an

⁸ https://files.consumerfinance.gov/f/documents/cfbp_debt-collection-NPRM.pdf

⁹ <https://www.theatlantic.com/health/archive/2019/08/medical-bill-debt-collection/596914/>

¹⁰ <https://www.theatlantic.com/health/archive/2019/08/medical-bill-debt-collection/596914/>

¹¹ <https://www.theatlantic.com/health/archive/2019/08/medical-bill-debt-collection/596914/>

¹² The FTC has a role in the enforcement of HIPAA under the Federal Trade Commission Act’s consumer protection prohibition against acts that are considered “unfair” or “deceptive.” According to a report published by HHS on “Examining Oversight of the Privacy and Security of Health Data Collected by Entities Not Regulated by HIPAA,” this role could include enforcement under practices that “could include, for example, failing to comply with an entity’s own privacy policy, deceptively failing to disclose material information about the use of personally identifiable information, or failing to reasonably secure this information.”

¹³ <https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html>

¹⁴ <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>

¹⁵ 42 USC 1320d-8

¹⁶ https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

¹⁷ https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

insurance company would be considered a business associate. As you know, such business associates must enter into a Business Associate Agreement with the covered entity regarding the protected health information to which they would have access and the terms and conditions of that access.¹⁸ The covered entity and the business associate are both required to comply with the requirements of the HIPAA Privacy Rule, including rules around sharing patient information with unauthorized individuals and sending information through a secure platform.

For such entities, the use of social media platforms without a patient's prior consent appears likely to constitute an unauthorized breach of protected health information. The social media messaging services on these platforms likely do not meet HIPAA's security requirements and these platforms likely do not have a business associate agreement in place with each and every covered entity or business associate using their services.

Further, many social media applications allow users to message other users based only on their name. Yet there may be many people with the same name as the patients sought by debt collectors, meaning debt collectors that use these services may be unlawfully sharing patients' private health information with the wrong person. When I searched myself on LinkedIn, I received results for one thousand and ninety-six Katie Porters. I certainly would not knowingly authorize my health care providers to share my protected health information with more than a thousand strangers, but this proposed rule effectively makes that permissible.

The proposed rule also allows debt collectors to use text messages as a form of communication, however there are few circumstances in which SMS text messaging can be HIPAA compliant. Most covered entities instead choose to prohibit texting protected health information, namely, the recipient of the text has to agree to receive this form of unsecured communications.¹⁹ Contrary to medical debt collectors, most covered entities choose to prohibit texting protected health information unless the recipient of the text has to agree to receive this form of unsecured communication.²⁰ Consent validates the accurateness of both the phone number and the individual before further information may or may not be disclosed. Under the proposed rule, an individual could be prevented from communicating by text with their physician about their health in a life-threatening situation— while receiving unlimited texts from debt collectors related to their treatment costs. In 1996, SMS did not exist, and therefore the HIPAA exemption for debt collection could not possibly have contemplated SMS as form of communication about an individual's private health information without the individual's consent.

For example, one consumer informed the CFPB in a February 2019 complaint that they had received multiple text messages about a medical debt that included specific information about their medical care even though: **“this company had in no way actually verified my phone number and could have been disclosing this information to anyone.”**²¹

¹⁸ 45 CFR 164.504(e)(2)

¹⁹ <https://www.hipaajournal.com/is-text-messaging-hipaa-compliant/>

²⁰ <https://www.hipaajournal.com/is-text-messaging-hipaa-compliant/>

²¹ <https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/3153601>

In another consumer complaint submitted to the CFPB, a patient complained that a debt collection agency pursuing payment for medical bills not only texted him about the debt but also aggressively pursued information regarding his health insurance company.²²

The CFPB's proposed rule may allow multiple violations of the HIPAA Privacy Law, and any exemptions for debt collection within HIPAA itself were granted 23 years ago, before cell phones, social media, and SMS texting even existed. Therefore, I ask that your agencies collaborate to conduct—and make public—a formal review of the privacy, health, and financial privacy implications of this proposed regulation and incorporate the results into any final rulemaking. Additionally, I ask that you please respond to the following questions by March 6, 2020:

1. Director Kraninger and Secretary Azar, did any HHS and CFPB coordination take place before the publication of the rule to ensure that protected health information was kept private and secure? If so, please summarize these efforts.
2. Director Kraninger, have you completed any analysis of the impact that the proposed rule would have on the privacy of patients' health information, particularly with respect to the use of social media and SMS texting?
3. Secretary Azar, considering that Section 1179 has yet to be clarified through regulations and is now out-of-date, will you commit to promulgating appropriate guidance or regulation to ensure the privacy and security of patients' health data in our 21st century technology environment?

Thank you for your time, and I look forward to continuing to discuss this important issue with you.

Very Truly Yours,



Rep. Katie Porter

²² <https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/3351517>