DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Center for Consumer Information and Insurance Oversight
200 Independence Avenue SW
Washington, DC 20201

April 5, 2022

Deputy Commissioner of Insurance Kevin Gaffney
Vermont Department of Financial Regulation
89 Main Street
Montpelier, VT 05620

Dear Deputy Commissioner Gaffney:

Following the Centers for Medicare & Medicaid Services (CMS) letter of December 22, 2021, and many productive conversations between your staff and CMS, this collaborative enforcement agreement describes our respective roles regarding enforcement of certain provisions of the Public Health Service Act (PHS Act), as extended or added by the Consolidated Appropriations Act, 2021 (CAA) in Vermont. Specifically, this agreement governs enforcement of section[s] 2719 (as applied by section 110 of the No Surprises Act), 2746 (other than section 2746(c)), 2799A-1, 2799A-2, 2799A-3, 2799A-4, 2799A-5, 2799A-7, and 2799A-9 (other than section 2799A-9(a)(4)) of the PHS Act with respect to health insurance issuers; sections 2799B-1, 2799B-2, 2799B-3, 2799B-8, and 2799B-9 with respect to health care providers and facilities; section 2799B-5 with respect to providers of air ambulance services; and sections 2799B-6 and 2799B-7 with respect to health care providers, facilities, and providers of air ambulance services (specified PHS Act provisions)[1].

In general, with regard to the specified PHS Act provisions, we have agreed that the Department of Financial Regulation (DFR) will perform the health insurance issuer compliance functions of policy form review, investigations and market conduct examinations, and consumer assistance. We have further agreed that the DFR will perform the provider, facility, and provider of air ambulance services compliance functions of consumer assistance and investigations. While this agreement is in place, CMS will undertake formal enforcement action against a health insurance issuer, provider, facility, or provider of air ambulance services with respect to the requirements outlined in this agreement only in the event that the DFR is unable to obtain compliance, to the extent CMS determines such action is warranted.

[1] This letter does not address or change the enforcement roles already established with respect to other federal requirements in title XXVII of the PHS Act. This letter does not address the roles with respect to federal requirements added by the CAA to title XXVII of the PHS Act other than the specified PHS Act provisions identified above.

I. Enforcement Roles

Policy Form Review

The DFR will review policy forms and other materials required to be filed with the DFR prior to use by health insurance issuers in Vermont in connection with individual and group health insurance coverage. The DFR will disapprove any form filed or withdraw any previous approval if the form is determined to not comply with the specified PHS Act provisions or applicable state requirements. If a health insurance issuer fails to amend its filing to comply with the specified PHS Act provisions as directed by the DFR, the DFR will refer the matter to CMS and will forward to CMS the noncompliant filing. Thereafter, CMS will take enforcement action as it determines appropriate and notify the DFR of any enforcement action it takes, including the results thereof.

Consumer Assistance

The DFR will provide consumer assistance by responding to consumer inquiries and complaints related to health insurance issuer, provider, facility, and provider of air ambulance services compliance with the specified PHS Act provisions in the same manner in which it responds to other health care consumer inquiries and complaints. In the event that the DFR discovers that a health insurance issuer, provider, facility, or provider of air ambulance services has acted in a manner that is not consistent with the specified PHS Act provisions, the DFR will request that the health insurance issuer, provider, facility, or provider of air ambulance services address and resolve the inquiry or complaint.

In the event a health insurance issuer, provider, facility, or provider of air ambulance services refuses to take corrective action to resolve an inquiry or complaint within the timeframe specified by the DFR, the DFR will, within three business days of such refusal, forward to CMS a copy of the inquiry or complaint, and any related materials. Thereafter, CMS will take enforcement action as it determines appropriate and advise the DFR of any enforcement action it takes, including the results thereof.

Investigations and Market Conduct Examinations

The DFR may perform an investigation or targeted market conduct examination specifically to identify potential noncompliance with the specified PHS Act provisions by a health insurance issuer, provider, facility, or provider of air ambulance services, or may include a review of compliance with the specified PHS Act provisions in an investigation or market conduct examination that is being conducted to also assess compliance with applicable state law.

The DFR will report to CMS regarding the scope and results of any investigation or market conduct examination related to the specified PHS Act provisions. This includes providing CMS with copies of all findings and draft reports for its investigations and market conduct examinations that include an assessment of compliance with the specified PHS Act provisions within 10 business days of finalization. CMS agrees to treat this information as confidential to the extent such protection is consistent with applicable federal law. Based on the findings of

these investigations, market conduct examinations, and any other information the DFR provides, CMS, after consultation with the DFR, may undertake further investigations and formal enforcement actions if CMS determines such action is warranted. In addition, CMS may continue to conduct investigations and market conduct examinations if CMS determines such actions are necessary, and will keep the DFR informed of such action consistent with Section II of this enforcement agreement.

If the DFR has evidence or information suggesting noncompliance with the specified PHS Act provisions by a health insurance issuer, provider, facility, or provider of air ambulance services, and the DFR determines that it will not investigate or conduct a targeted market conduct examination, within three business days of making such a decision the DFR will confer with CMS about its decision not to examine the health insurance issuer, provider, facility, or provider of air ambulance services and the reasons for its decision. CMS reserves the right to conduct investigations and targeted market conduct examinations in Vermont pursuant to sections 2723 and 2799B-4 of the PHS Act and 45 C.F.R. part 150, as applicable, if CMS determines such action is warranted. CMS will consult with the DFR before initiating any investigation of a provider, facility, or provider of air ambulance services under section 2799B-4 of the PHS Act or any investigation or market conduct examination of an issuer related to compliance with specified PHS Act provisions in the state.[2]

II. CMS's Commitment to Keep the Department of Financial Regulation (DFR) Informed of the Agency's Enforcement Activities

As part of this collaborative enforcement agreement, CMS will keep the DFR informed of significant developments with respect to any PHS Act enforcement actions brought against health insurance issuers, providers, facilities, and providers of air ambulance services in Vermont to the extent such communication is not otherwise prohibited by law. This will be done through communication with a person or persons designated by the DFR. Further, the DFR will keep CMS informed of developments of which it becomes aware that may impact compliance with the specified PHS Act provisions through communication with the person or persons designated by CMS.

III. Exchange of Information and Maintenance of Confidentiality

To facilitate the DFR's efforts under this collaborative enforcement agreement, the DFR may gain access to confidential information, personally identifiable information, and protected health information from CMS. The DFR must treat this information as confidential and subject to the restrictions on uses and disclosure under Title 8 V.S.A. section 22 and the HIPAA Standards for Individually Identifiable Health Information (the Privacy Rule) at 45 CFR Part 160 and Subparts

[2] The process by which CMS would investigate complaints and impose civil money penalties against providers, facilities, and providers of air ambulance services is discussed in a notice of proposed rulemaking entitled, *Requirements Related to Air Ambulance Services, Agent and Broker Disclosures, and Provider Enforcement* (86 FR 51730), published September 16, 2021.

A and E of Part 164 that would apply to a covered entity, regardless of the DFR's status under HIPAA. The Deputy Commissioner will maintain documents received from federal law enforcement and regulatory agencies as confidential and privileged under the DFR's authority. This agreement, if signed by the designated State representative, constitutes an assurance of confidentiality by the DFR.

Certain documents, data, templates, and other forms of information contained within the Health Insurance Oversight System (HIOS) have been deemed confidential by CMS or by the sources of the information within HIOS. This includes, but is not limited to, data or other information relating to Qualified Health Plans (QHPs) that the DFR may receive from CMS or may access via HIOS. The DFR agrees to use such data or information only for purposes of the DFR regulation and oversight in Vermont consistent with the purposes of this agreement and the HIOS Rules of Behavior (Addendum), and that any data deemed confidential or privileged by CMS shall not be publicly disclosed, nor disseminated beyond the individuals authorized by the DFR, and shall not constitute a waiver of any privilege or claim of confidentiality.

Should the DFR discover that any confidential information subject to this agreement is lost, stolen, disclosed or accessed in a manner inconsistent with this agreement, the DFR affirms that it will report the incident or breach by email to both the CMS IT Service Desk (cms_it_service_desk@cms.hhs.gov) and CCIIO's Compliance and Enforcement Division (marketconduct@cms.hhs.gov) within one hour of discovery, and cooperate fully in the federal security incident response.[3] When reporting the incident, the DFR will be required to provide contact information, data file information, and data dissemination information for this purpose.

To facilitate enforcement by CMS if the DFR is unable to obtain voluntary compliance, the DFR will provide working documents and information obtained while seeking compliance to CMS. CMS will maintain the confidentiality of the records consistent with the applicable system of records, "Complaints Against Health Insurance Issuers and Health Plans (CAHII)," 09-70-0516.[4]

If either the DFR or CMS enters into relationships with third parties to assist with its duties under this agreement, it must execute contracts that require such entities and any subcontractors or affiliates of such entities to comply with the confidentiality and limitations on disclosure requirements described herein.

IV: Terms and Duration of Collaborative Enforcement Agreement

This collaborative enforcement agreement may be modified as necessary to ensure that residents of Vermont are receiving the full protections established by the specified PHS Act provisions. The above terms, as presently written or as modified in the future, will apply for as long as CMS has primary enforcement responsibility for the specified PHS Act provisions in Vermont. CMS will enter into discussions with the DFR to ensure an effective transition to state enforcement,

[3] See https://osec.doc.gov/opog/privacy/Memorandums/OMB_M-17-12.pdf for additional details regarding data incident notification.

[4] See https://www.federalregister.gov/documents/2007/05/08/E7-8757/privacy-act-of-1974-report-of-a-modified-or-altered-system-of-records for additional details.

pursuant to 45 C.F.R. § 150.221, if and when the circumstances requiring CMS enforcement under 45 C.F.R. § 150.203 no longer apply.

We appreciate your willingness to collaborate with us on the enforcement of the specified PHS Act provisions, and we look forward to working with you to ensure that the residents of Vermont receive all the benefits of these important consumer protections.

Samara A. Lorenz -S
Digitally signed by Samara A. Lorenz -S
Date: 2022.04.19 15:42:58 -04'00'

Samara Lorenz
Director, Oversight Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

Kevin Gaffney
Deputy Commissioner of Insurance
Vermont Department of Financial Regulation

Addendum

HIOS Rules of Behavior

Introduction

The HIOS Rules of Behavior (ROB) provides common rules on the appropriate use of the HIOS system and its data. The HIOS ROB applies to all HIOS users, including, but not limited to, insurance carriers, HHS staff, HHS contractors, States, and other Federal agencies.

All HIOS users must read these rules before accessing the HIOS system and its data.

The HIOS ROB applies to both the local and remote use of HIOS information (in both electronic and physical forms) and the HIOS system by any individual.

HHS reserves the right to deny access to HIOS and/or to take other appropriate action in the event that these rules are not followed and adhered to by HIOS users and the organizations that they represent.

HIOS users shall:

- Comply with HHS and Department policies and standards and with applicable laws in the use of both HIOS information and system's functionality.
- Use provisions for access restrictions and strictly prohibit the sharing of accounts.
- Only access sensitive HIOS information necessary to perform job functions (i.e., need to know).
- Log-off or lock systems when leaving them unattended.
- Report all known or suspected security incidents, known or suspected information security policy violations or compromises, or suspicious activity to the Marketplace Service Desk (MSD) immediately. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information, including Personally Identifiable Information (PII), maintained by or in possession of HHS.
- Secure sensitive HIOS information (on paper and in electronic formats) when left unattended.
- Keep sensitive HIOS information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive HIOS data when no longer needed.

- Prevent unauthorized disclosure or modification of sensitive HIOS information resident in HIOS.
- Ensure that passwords conform to the requirements set forth by HHS for HIOS.
- Maintain passwords that are committed to memory or stored in a secure place.

HIOS users shall not:

- Share their HIOS account, identity, or password or use another person's account, identity, or password.
- Attempt to exceed authorized access to sensitive HIOS information.
- Direct or encourage others to violate HHS and Departmental policies.
- Circumvent security safeguards or reconfigure systems (i.e., violation of least privilege).
- Store sensitive HIOS information in public folders or other insecure physical or electronic storage locations.
- Share sensitive HIOS information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, download, or present (e.g., training, webinar) sensitive HIOS information, unless such action is explicitly permitted by the manager or owner of such information.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.

Conclusion

Violations of the HIOS Rules of Behavior or other information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities. In addition, violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HIOS Rules of Behavior draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.