DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Special Reviews

OFFICE OF INFORMATION AND TECHNOLOGY
VETERANS HEALTH ADMINISTRATION

False Statements and Concealment of Material Information by VA Information Technology Staff

ADMINISTRATIVE INVESTIGATION | REPORT #17-01980-201 | JANUARY 28, 2021

MISSION

The mission of the Office of Inspector General is to serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

The VA Office of Inspector General (OIG) conducted an administrative investigation in response to a joint referral received in December 2016 from the then under secretary of health and the then assistant secretary for information and technology and chief information officer to investigate whether certain VA employees had conflicts of interest in connection with VA's establishment of a cooperative research and development agreement (CRADA) with Flow Health, Inc. (Flow Health). A CRADA is an agreement between a federal laboratory and nonfederal party, such as a private company or university, to collaborate on research and development.[1] Within VA, the Veterans Health Administration (VHA) has traditionally been the entity that has entered into CRADAs with private industry and universities. In this instance, the stated objective of the research collaboration established by the CRADA was to "help VA improve the health and wellness of veterans." This objective would be accomplished by using VA health data along with Flow Health's deep learning and artificial intelligence resources to discover evidence to prevent disease onset, improve the precision of diagnoses, and identify treatment plans that together position clinicians to make recommendations tailored specifically for individual veteran patients.

On October 28, 2016, the VA Office of Information and Technology (OIT) executed a CRADA with Flow Health, titled "Build a Medical Knowledge Graph with Deep Learning to Inform Medical Decision-Making and Identify Evidence to Prevent Disease Onset, Make Previously Unrecognized Diagnoses, and Personalize Treatments." The CRADA contemplated VA sharing with Flow Health the health data of all veterans who had ever received health care from VA, including the genomic information of veterans maintained by VA's Million Veteran Program.[2] In addition to preexisting records, the agreement called for continuing to provide Flow Health with veterans' current health data for five years.[3]

Media coverage of a Flow Health press release alerted senior VHA and OIT officials to the existence of the CRADA on or about November 30, 2016. VA unilaterally terminated the CRADA on December 20, 2016, before any health data was given to Flow Health.

[1] The authority to enter into a CRADA with a nonfederal research partner is found in Section 2 of the Federal Technology Transfer Act of 1986, 15 U.S.C. § 3710a.

[2] The Million Veteran Program is a national research project sponsored by the VHA Office of Research and Development to learn how genes, lifestyle, and military exposures affect health and illness. "About the Million Veteran Program," VHA Office of Research and Development, accessed January 6, 2021, https://www.mvp.va.gov/webapp/mvp-web-participant/#/public.

[3] The CRADA defined health data to include "clinical (structured and unstructured data), claims, pharmacy, laboratory, radiology, pathology, diagnostic, patient-generated and molecular data (e.g., microbiome, DNA, RNA, proteomics) with Individually Identifiable Information allowing the integration of VA data with external individually identifiable data sets (e.g., health data from commercial payers and providers)." It also included veterans' genomic data maintained by VA.

The CRADA identified an OIT program manager (OIT program manager) as the "CRADA Leader" and a health system specialist in the VHA central office (VHA employee) as the "VA Principal Investigator."[4] The OIG did not substantiate that any of the employees named in the complaint had a financial interest in Flow Health that would create a conflict of interest under relevant law.[5]

The OIG did substantiate, however, that the OIT program manager and the VHA employee made false representations to and concealed material information from the VA approving official for the CRADA. Prior to the approval of the CRADA, three VA privacy experts informed the OIT program manager and the VHA employee that the terms of the proposed CRADA raised serious concerns that needed to be addressed before the CRADA could be approved. Despite the objections from these experts, the OIT program manager and the VHA employee failed to disclose the unresolved privacy issues to the approving official. They falsely represented that all reviews—including privacy, information security, and legal—had been completed and implied that any resulting identified issues had been addressed and resolved. The OIG concluded that the approving official relied on the information received from the OIT program manager and the VHA employee and was led to approve the CRADA under false pretenses. As a result of the OIT program manager's and the VHA employee's actions, the health data of tens of millions of veterans would have been placed at risk of disclosure had the contract not been cancelled.[6]

The OIG referred this matter to the U.S. Department of Justice, which declined to prosecute. The OIG made two recommendations to VA related to determining what administrative action, if any, should be taken with respect to the OIT program manager's and the VHA employee's conduct. In response to this report, VA concurred with all recommendations. The entirety of VA's response can be found in appendix C.

R. JAMES MITCHELL, ESQ.
Acting Assistant Inspector General
for the Office of Special Reviews

[4] The CRADA defined "Principal Investigator" as: "the VA Employee who actually conducts the basic research in accordance with the Statement of Work, i.e., under whose immediate direction the research is conducted or, in the event of research conducted by a team of investigators, is the responsible leader of that team." The original complaint received by the OIG also identified two other individuals, but the OIG did not identify any potential misconduct with respect to these employees.

[5] See 5 C.F.R. § 2635, subpart D; 18 U.S.C. § 208(a).

[6] The OIG was unable to determine why the OIT program manager and the VHA employee engaged in this conduct.

Contents

Abbreviations

ASD	Architecture, Strategy and Design (The Office of)
BAA	Business Associate Agreement
CRADA	Cooperative Research and Development Agreement
HIPAA	Health Insurance Portability and Accountability Act
ISO	Information Security Officer
MVP	Million Veteran Program
OAR	Office of Accountability and Review
OGC	Office of General Counsel
OIG	Office of Inspector General
OIS	Office of Information Security
OIT	Office of Information and Technology
ORD	Office of Research and Development
PHI	Protected Health Information
PII	Personally Identifiable Information
VA	Department of Veterans Affairs
VHA	Veterans Health Administration

Introduction

The VA Office of Inspector General (OIG) conducted an administrative investigation in response to a joint referral received in December 2016 from the then under secretary for health and the then assistant secretary for information and technology and chief information officer to investigate whether certain VA employees had conflicts of interest in connection with VA's establishment of a cooperative research and development agreement (CRADA) with Flow Health. A CRADA is an agreement between a federal laboratory and nonfederal party, such as a private company or university, to collaborate on research and development.[7] In this instance, the stated objective of the research collaboration established by the CRADA was to "help VA improve the health and wellness of veterans." This objective would be accomplished by using VA health data along with Flow Health's deep learning and artificial intelligence resources to discover evidence to prevent disease onset, improve the precision of diagnoses, and identify treatment plans that together position clinicians to make recommendations tailored specifically for individual veteran patients.

A program manager in the Office of Information Technology (OIT) (OIT program manager) and a health system specialist in the Veterans Health Administration (VHA) central office (VHA employee) were identified as having been involved in the CRADA.[8]

In the course of its investigation, the OIG interviewed the OIT program manager, the VHA employee, the approving official, the VHA chief health technology officer, and the deputy chief counsel of the Office of General Counsel (OGC) Health Care Law Group. In addition, the OIG reviewed transcripts of sworn testimony of VA employees obtained by the former VA Office of Accountability Review (OAR) during an administrative investigation board of inquiry into the Flow Health CRADA.[9] The OIG also reviewed CRADA documentation, VA email records, non-VA email and text message records, telephone records, official personnel records, and subpoenaed financial (bank) records. Additionally, the OIG reviewed applicable federal laws,

[7] The authority to enter into a CRADA with a nonfederal research partner is found in Section 2 of the Federal Technology Transfer Act of 1986, 15 U.S.C. § 3710a.

[8] The original complaint received by the OIG also identified the VHA employee's supervisor, the VHA chief health technology officer and the approving official, the deputy chief information officer for the Office of Architecture, Strategy and Design (ASD) within OIT, as being involved with the establishment of the Flow Health CRADA. However, the OIG found that the VHA employee's supervisor was not involved with the CRADA, other than having a general knowledge that the VHA employee was working with the OIT program manager to establish a research collaboration between the OIT and Flow Health, and the OIG found that the approving official approved the CRADA based on the misrepresentations of the OIT program manager and the VHA employee.

[9] In February 2017, the OAR conducted an administrative investigation to determine whether staff from the OIT ASD entered into a CRADA with Flow Health "without proper authorization." The OAR was unable to determine whether ASD had authority to enter into the CRADA, and stated in its report that it was unclear whether the CRADA related "to technology transfer or crossed into the line of VHA collaborative research and development." On June 12, 2017, the OAR's staff was reassigned to the VA Office of Accountability and Whistleblower Protection, and the OAR was discontinued.

regulations, and VA policy. For more information on the OIG's scope and methodology, see appendix A. The OIG referred this matter to the U.S. Department of Justice, which declined to prosecute.

The OIT Office of Architecture, Strategy and Design

The OIT Office of Architecture, Strategy and Design (ASD) was established in August 2010.[10] ASD's mission was to plan, design, and drive IT-enabled transformation efforts across the department to improve veteran access to VA services. In carrying out this mission, ASD performed research and development related to information technology. In April 2015, the then VA Secretary designated ASD as a federal research laboratory with authority to enter into CRADAs under the Federal Technology Transfer Act of 1986. As the head of ASD, the deputy chief information officer had the statutory authority to execute CRADAs on behalf of VA.[11] In January 2016, the deputy chief information officer established a VA CRADA program manager position within ASD to support its research and development efforts.

Historically, research and development activities in VA had been associated with the provision of medical care to veterans and had been overseen by the VHA Office of Research and Development (ORD). The ORD has comprehensive policies governing its research activities, including guidance on the use of CRADAs. VA established research laboratories, such as ASD, with authority to enter into CRADAs under the Federal Technology Transfer Act.[12] These laboratories' research activities, including their CRADA activities, were outside the purview of the ORD. Accordingly, ORD policies governing CRADAs did not apply to ASD or any other VA research laboratory established independently of the VHA ORD.[13]

The OIT Program Manager

In March 2016, the OIT program manager became the CRADA's program manager and he reported to the deputy chief information officer. The OIT program manager's duties and responsibilities included (1) seeking opportunities to use CRADAs; (2) vetting potential CRADA partners; (3) negotiating statements of work on behalf of VA; (4) ensuring the protection of VA information; (5) facilitating all necessary reviews and recommendations of a proposed CRADA; and (6) providing accurate guidance concerning technology transfer laws, intellectual property rules, and VA's federal technology sharing policies. In 2017, the OIT program manager was reassigned to the OIT Account Management Office, and as of January 6, 2021, continued to work in that office.

[10] In February 2018, ASD was dissolved through an OIT reorganization. ASD's designation as a federal laboratory and authority to execute CRADAs was not assumed by any other OIT office.

[11] 15 U.S.C. § 3710a.

[12] 15 U.S.C. § 3710a.

[13] ASD had no policies or procedures governing CRADAs.

The VHA Employee

In May 2013, the VHA employee became VHA's deputy chief health technology officer. He reported to the VHA chief health technology officer. In this position, the VHA employee's job responsibilities included identifying and testing emerging medical solutions and technology and communicating those opportunities in writing to a range of clinical and managerial leaders and personnel in clinical program offices in VHA. As of January 6, 2021, the VHA employee continued to work as VHA's deputy chief health technology officer.

The Flow Health CRADA

On October 28, 2016, ASD entered into a CRADA with Flow Health. The CRADA project was titled, "Build a Medical Knowledge Graph with Deep Learning to Inform Medical Decision-Making and Identify Evidence to Prevent Disease Onset, Make Previously Unrecognized Diagnoses, and Personalize Treatments." Under the terms of the CRADA, ASD committed VA to provide Flow Health access to the health data of tens of millions of veterans. VHA and OIT senior leaders first learned about the CRADA through media coverage of a press release issued by Flow Health announcing the CRADA.[14] Jointly, VHA and OIT senior leaders unilaterally terminated the CRADA on December 20, 2016, before any veterans' health data was disclosed to Flow Health.

The idea for the CRADA originated during a meeting between the VHA employee and the Chief Executive Officer of Flow Health (Flow Health CEO) on March 16, 2016. During this meeting, the VHA employee and the Flow Health CEO discussed the development of a CRADA that would provide Flow Health access to all available VA health data to support Flow Health's "machine learning/artificial intelligence work." On June 7, 2016, the VHA employee enlisted the assistance of the OIT program manager with establishing the CRADA and provided a draft statement of work to him. Between June 2016 and October 2016, text message and email records show that the VHA employee, the OIT program manager, and the Flow Health CEO collaborated on creating the CRADA, which was eventually signed by the approving official on October 28, 2016.

[14] On November 29, 2016, Flow Health issued a press release containing a reproduction of the Official Seal of the Department of Veterans Affairs followed by the slogan, "VA HEALTHCARE – Defining EXCELLENCE in the 21st Century." Flow Health, news release, "Bringing Artificial Intelligence to the Veterans Health Administration," Nov. 29, 2016. Flow Health's inclusion of the VA seal and the VA slogan at the top of the press release violated the terms of the CRADA, which stated that Flow Health "shall not state or imply that the Government or any of its organizational units or employees endorses any product or service."

Finding and Analysis

Finding: The OIT Program Manager and the VHA Employee Made False Representations to and Concealed Material Information from the CRADA Approving Official

The proposed CRADA with Flow Health required authorization by the approving official. In late September 2016, prior to signing the CRADA, the approving official requested an explanation of the cybersecurity implications of the proposed CRADA. Over the course of the next month, the OIT program manager and the VHA employee made false statements to the approving official pertaining to the status of the information security and privacy reviews of the CRADA and a Business Associate Agreement (BAA), an ancillary document to the CRADA. The OIT program manager and the VHA employee also concealed from the approving official significant privacy concerns raised by subject matter experts. The evidence indicates that between September 27, 2016, and October 27, 2016, the OIT program manager and the VHA employee collectively made multiple false statements to the approving official and advocated that he execute the CRADA while concealing from him material information pertaining to the significant unresolved concerns of VA privacy experts. These statements included false representations that all reviews, including privacy, information security, and legal, had been completed—implying that any identified issues had been addressed and resolved.[15]

The OIT program manager and the VHA employee never disclosed to the approving official that multiple individuals had raised privacy and security concerns about the CRADA that, as discussed below, had never been fully addressed. On October 28, 2016, relying on the representations made by the OIT program manager and the VHA employee and believing that the CRADA had been reviewed and that all privacy and security concerns had been resolved, the approving official signed the CRADA. In his interview, the approving official told the OIG investigator, "Everybody that I thought was supposed to … said it looked fine, and that's why I signed the CRADA." The approving official also told the OIG investigator that neither the OIT program manager nor the VHA employee told him of any concerns, and said that, if he had been told of the concerns, "I think that would have led me in a different direction. I believe it would have caused me to get on the phone either with them or with [others] and say, what's the issue here, and let's get this worked out."

Privacy and Security Concerns

Between June 2016 and October 2016, multiple individuals raised privacy and security concerns about the CRADA.

[15] The OIG was unable to determine why the OIT program manager and the VHA employee engaged in this conduct.

Contract Employee

In June 2016, the VHA employee provided the OIT program manager with a draft statement of work for a proposed CRADA with Flow Health. The OIT program manager provided the statement of work to a contract employee assigned to ASD's CRADA Program Office. The contract employee reviewed the statement of work and replied to the OIT program manager:

> Took a look at the [statement of work] you provided – a very intriguing idea! However, I would be remiss in my responsibilities to VA if I didn't caution about security issues introduced by the characteristics of this CRADA. We can certainly talk more about these, but in short the integration of large data sets of [Protected Health Information (PHI)], compounded by computation in a cloud environment, introduce a number of regulatory and statutory security challenges. Interestingly, I suspect that the challenges will be very similar to the challenges faced by VA's own GENISIS initiative.

VA's Attorneys Identified Potential Privacy Issues

In late August 2016, the OIT program manager sought legal review of the proposed CRADA. The review was conducted by the deputy chief counsel of a specialty team in the VA Office of General Counsel Health Care Law Group. In addition to her review, the deputy chief counsel asked another VA attorney who specialized in information law to review the proposed CRADA. In a subsequent email dated September 13, 2016, that attorney told the deputy chief counsel, "I know VHA has been very concerned with the re-identification of even de-identified data under the Health Insurance Portability and Accountability Act (HIPAA) safe harbor. So, this is definitely one that needs to be routed through VHA Privacy."

The deputy chief counsel told the OIG that she verbally informed the OIT program manager that the proposed CRADA needed to be reviewed by the VHA privacy officials. The deputy chief counsel told OIG investigators that the OIT program manager indicated to her that the VHA employee had already coordinated with the VHA privacy officials and they were comfortable with it. On September 15, 2016, the deputy chief counsel completed her legal review of the CRADA.

The OIG found no evidence that, as of September 15, 2016, the VHA privacy officials had ever received, reviewed, or approved the CRADA. To the contrary, the VHA privacy officer first learned of the proposed CRADA on or about October 5, 2016, and, rather than approving the CRADA, the evidence indicates that the VHA privacy officer had "various privacy concerns" about it.

VA Privacy Officials Identified Potential Privacy Issues with the Proposed CRADA

On October 4, 2016, the OIT program manager emailed the proposed CRADA to the then executive director of OIT Enterprise Cybersecurity Strategy (the executive director) and asked him to provide "any suggested comment in relation to privacy." On October 5, the executive director replied to the OIT program manager and connected him via email with the then associate deputy assistant secretary for OIT Policy, Privacy, and Incident Response (the OIT privacy official). The OIT program manager replied to the executive director and the OIT privacy official (copying the approving official and the VHA employee), stating,

> Actually, our OGC and [Office of Information Security (OIS)] have reviewed and approved the CRADA including privacy related items. Keeping this focused, [the approving official] asked for your feedback from a security perspective if any. If you have any comment today we appreciate it.

On October 5, 2016, the OIT privacy official responded to the OIT program manager (copying the approving official, the VHA employee and the executive director), stating,

> I would like the Privacy team to have a look at this – we are currently in a tussle with [another federal agency] regarding privacy related to the Million Veteran Program and rather than deal with any potential aftermath I would like to head off any issues before they occur. Adding Privacy.[16]

On October 6, 2016, the OIT program manager removed the approving official from the email thread and replied to the OIT privacy official (copying the executive director and the VHA employee). The OIT program manager told the OIT privacy official that he had worked with OGC and OIS to put together the related BAA that would enforce HIPAA regulations and that he had "the necessary requirements in place to move forward."[17]

Contrary to the OIT program manager's assertions to the executive director and the OIT privacy official, the OIS review did not include privacy-related matters, nor did it result in an approval of the CRADA. The OIS review that the OIT program manager referenced in his October 5 email to the executive director and his October 6 email to the OIT privacy official was actually conducted by an information security officer (ISO) and was limited to the BAA. The ISO's "cursory" review focused on ensuring that the BAA contained the appropriate boilerplate language concerning *data breach prevention and data breach protocol*. In emails sent to the OIT program manager, the VHA employee and the Flow Health CEO on October 5, 2016, the ISO indicated

[16] After receiving this email from the OIT privacy official, the OIT program manager forwarded it to the VHA employee and the Flow Health CEO.

[17] After replying to the OIT privacy official's email, the OIT program manager forwarded a copy of his reply to the Flow Health CEO.

that, other than language regarding VA's right to conduct random and/or routine HIPAA Privacy, Security and Breach Notification audits, which she was continuing to research, the rest of the BAA looked "fine" from the ISO's perspective. The ISO advised the OIT program manager and the VHA employee to submit the BAA to the deputy chief counsel for review and approval. The OIT program manager then sent the BAA to the deputy chief counsel as an "FYI."[18] The OIG has found no evidence that the deputy chief counsel responded to this email or approved the BAA.

Subsequently, on October 6, the OIT privacy official replied to the OIT program manager (copying the VHA employee and the executive director, and adding the director of the VHA Information Access and Privacy Program Office (the VHA privacy officer).[19] In his email, the OIT privacy official stated,

> I appreciate [the] opportunity to look this over and comment. Below are the observations of our team and some of the areas of concern they raised. In addition to our folks, I've included VHA's Privacy Officer . . . for her awareness. Its [*sic*] been my experience in working with [the Million Veteran Program (MVP)], that efforts involving research present unique challenges that require additional scrutiny. I would much rather err on the side of caution when dealing with PII/PHI. That being said, we are available, as I'm sure VHA Privacy is, to work with anybody to address the issues we've raised.

The OIT privacy official's email identified the issues raised by the proposed CRADA, including the need to dedicate privacy staff to the project to ensure oversight given the ongoing transfers of large quantities of personally identifiable information (PII) and personal health information (PHI) contemplated by the CRADA. In addition, the OIT privacy official observed that the statement of work failed to require training of Flow Health's staff on VA privacy and information security requirements before being given access to VA PII and PHI. Commenting on the BAA, the OIT privacy official pointed out that it did not conform to the template posted on VHA's data portal and recommended that the OIT program manager use the compliant VHA BAA.[20]

After receiving the OIT privacy official's email, the OIT program manager replaced the original BAA with the VHA BAA. Later the same day, the OIT program manager sent the Flow Health CEO and the VHA employee the VHA BAA template. The Flow Health CEO signed the VHA

[18] The OIT program manager's email did not specifically request that the deputy chief counsel "review and approve" the BAA as the ISO had instructed in her email. In his email to the deputy chief counsel, the OIT program manager stated, "FYI sharing with you a copy of the draft BAA we have for Flow Health."

[19] The director of the VHA Information Access and Privacy Program Office's role and functional title was "VHA Privacy Officer."

[20] After receiving this email from the OIT privacy official, the OIT program manager forwarded it to the Flow Health CEO.

BAA dated October 6, 2016, and returned it to the OIT program manager and the VHA employee.[21] Other than obtaining the correct VHA BAA, the other privacy and information security concerns raised by the OIT privacy official were not addressed. Neither the OIT program manager nor the VHA employee responded to the OIT privacy official's October 6 email, nor did they inform the approving official of his analysis or concerns.

On October 12, 2016, the VHA privacy officer, having been copied on the OIT privacy official's October 6 email, sent the OIT program manager and the VHA employee an email advising them that she had privacy-related concerns about the proposed CRADA. In particular, the VHA privacy officer told the OIT program manager and the VHA employee that rules promulgated under HIPAA disallow the use and disclosure of PHI for research purposes unless the use and disclosure is authorized in accordance with HIPAA. The VHA privacy officer also told them that 45 CFR § 164.501 defined "research" as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge" and that any activity using VHA-owned PHI that met that definition was considered to be "research" regardless of whether the activity involved human subjects research. The approving official was not included in this email's distribution. Neither the OIT program manager nor the VHA employee responded to the VHA privacy officer's email, nor did they inform the approving official of her analysis and concerns.[22]

On October 12, 2016, the associate director of regulatory affairs for VHA ORD (the regulatory affairs official), having been copied by the VHA privacy officer on her earlier email, followed up with her own email to the OIT program manager and the VHA employee. The regulatory affairs official told the OIT program manager and the VHA employee that she had some "human subject protection issues" that needed to be addressed "based upon the [statement of work], including access to MVP health data by an external Collaborator based upon MVP's informed consent language." She further told them, "Regardless of whether or not this is human subjects research subject to IRB review and approval, human subjects research exempt from IRB review and approval, or non-human subjects research, [requires] VA Research and Development Committee approval … in addition to the applicable subcommittees."

Alarmed by the CRADA's commitment of research data from the MVP, the regulatory affairs official immediately contacted the MVP team and asked if they knew that the CRADA obligated the release of MVP program research data to Flow Health. The answer was no. The regulatory affairs official followed up her email with a telephone call to the OIT program manager. He did not answer so the regulatory affairs official left him a voice message telling him that he could not use MVP data and asked him to call her back. The OIT program manager and the VHA

[21] The OIT program manager did not send the VHA BAA to the ISO for review and approval until October 17, 2016. It was not until October 19, 2016, that the ISO gave her approval on the VHA BAA.

[22] On October 14, 2016, while on a call with the Flow Health CEO, the OIT program manager forwarded the VHA privacy officer's October 12, 2016 email to the Flow Health CEO.

employee did not respond to the regulatory affairs official, nor did they inform the approving official of her analysis or concerns.[23] During her interview with OAR investigators, the regulatory affairs official said that, in her experience, when she has written an email and made a call like she did here, "usually that raises the alarms and everything stops."

On October 28, 2016, the approving official executed the Flow Health CRADA—relying on multiple misrepresentations and assurances from the OIT program manager and the VHA employee indicating that it was ready to be signed and that they had obtained approval from privacy, security, and legal personnel.

The OIT Program Manager and the VHA Employee Made False Representations to and Concealed Material Facts from the Approving Official

Federal employees are obligated to carry out their duties honestly.[24] Between September 27, 2016, and October 27, 2016, the OIT program manager and the VHA employee collectively made multiple false statements to the approving official. They repeatedly told him that the CRADA was ready to sign and that privacy, information security, and legal reviews had been completed. However, the OIT program manager and the VHA employee had been advised of multiple privacy and security concerns that they did not convey to the approving official.

In addition, the OIT program manager removed the approving official from an email thread in which VA subject matter experts raised significant concerns and counseled that additional review of the CRADA was required and that they did not have permission to use MVP data. As a result, the approving official was never apprised of those concerns. These false representations and acts of concealment frequently occurred soon after or during communications with the Flow Health CEO. Appendix B contains a detailed chronology of the communications between the OIT program manager, the VHA employee, the Flow Health CEO, and the approving official.

Below are some examples of the false representations and concealment of material facts made to the approving official.

Example 1

In a memorandum attached to a September 27, 2016 email, the OIT program manager responded to a question that the approving official asked concerning the

[23] The OIT program manager told OIG investigators that he did not recall receiving the emails from the OIT privacy official, the VHA privacy officer, and the regulatory affairs official, or receiving a telephone voice message from the regulatory affairs official. When asked about forwarding some of these emails to the Flow Health CEO, the OIT program manager said that he had no recollection of forwarding them to the Flow Health CEO.

[24] This obligation arises in various applicable laws, regulations, and policies, such as 18 U.S.C. § 1001 (fraud or false statements in a government matter), the 5 C.F.R. § 2635 (standards of ethical conduct for employees of the executive branch); 5 C.F.R. § 735.203 (restrictions on conduct prejudicial to the government), and VA Directive 5025, *Legal*, April 15, 2002.

cybersecurity implications of the proposed CRADA. The OIT program manager told the approving official that, "The CRADA project proposal, patient data access and privacy implications, were [r]eviewed and approved by both VA OIS and OGC. This confirms the protection of patient data privacy and cybersecurity according to the CRADA document[.]"

The OIT program manager's statement to the approving official that "OIS" had reviewed and approved the CRADA was false because the OIS's information security officer did not review the CRADA for privacy issues. The OIT program manager's statement that "OGC" had reviewed and approved the CRADA was false because the deputy chief counsel's approval of the CRADA on September 15, 2016, was premised on the OIT program manager's misrepresentation to her that VHA privacy officials were comfortable with the CRADA. The VHA privacy officer did not become aware of the proposed CRADA with Flow Health until early October 2016. Moreover, upon learning of the proposed CRADA in early October, the VHA privacy officer raised significant concerns that were not fully addressed by the OIT program manager and the VHA employee. Telephone records reflect that the OIT program manager sent this email while on the telephone with the Flow Health CEO.

Example 2

On October 6, 2016, the OIT program manager emailed the approving official that "We completed the necessary reviews per our conversations and the CRADA is ready for your signature."

This statement was a concealment from the approving official of a material fact because, at the time the OIT program manager sent this email to the approving official, the OIT program manager knew that earlier that same day, the OIT privacy official had relayed to him (and to the VHA employee) several significant concerns regarding the proposed CRADA that had not been communicated to the approving official and had not been fully addressed. Telephone records reflect that the OIT program manager sent this email also while on the telephone with the Flow Health CEO.

Example 3

On October 11, 2016, the OIT program manager emailed the approving official with a copy to the VHA employee and Flow Health CEO, stating, "This is the Flow Health proposed CRADA, for your approval and signature. We completed a review and have concurrence on privacy and security."

This statement was false because, at the time the OIT program manager sent this email to the approving official, there was no concurrence by privacy and security officials. To the contrary, the OIT privacy official had raised a number of significant privacy concerns that had not been fully addressed. The OIT program manager's statement to the approving official that they had

concurrence on "security" was false because the ISO did not review the CRADA. In addition, these concerns had not otherwise been communicated to the approving official.

Example 4

On October 17, 2016, the VHA employee responded via email to questions raised by the approving official and assured him that, "Yes. OIS has reviewed and approved both the CRADA and the BAA."

The VHA employee's response to the approving official's third question, in which he stated, "Yes. OIS has reviewed and approved both the CRADA and the BAA," was false. First, the statement that the CRADA was approved by "OIS" was false because the ISO never approved the CRADA. Second, the statement that the BAA was approved by "OIS" was false because the ISO did not review and approve the VHA BAA until October 19, 2016.

The OIG did not find evidence of any financial relationship between the OIT program manager or the VHA employee and the Flow Health CEO or Flow Health more generally that would create a conflict of interest under relevant law.[25] Their conduct does, however, implicate various laws, regulations, and policies that require federal employees to conduct themselves honestly, in a manner that is not prejudicial to the government, and does not result in the misuse of their authorities.[26]

The OIT Program Manager and the VHA Employee Used Non-VA Email Accounts and Text Messaging Services to Conduct Official Business

Email and text messaging records obtained from Flow Health and Flow Health's sales agent revealed that both the OIT program manager and the VHA employee used personal email and text messaging accounts to communicate with the Flow Health CEO and Flow Health's sales agent concerning the CRADA. Federal law requires VA employees to use their official VA electronic messaging account or copy their official VA-issued electronic messaging account in the original creation or transmission of information related to the transaction of public business, such as the CRADA, or forward a complete copy of the record to their VA-issued electronic messaging account within 20 days.[27] The OIT program manager and the VHA employee failed to copy or forward all of their electronic communications regarding the CRADA to their respective VA accounts as required by law.

[25] 5 C.F.R. § 2635, Subpart D, or 18 USC § 208(a).

[26] See 5 C.F.R. § 735.203 ("An employee shall not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the Government"); 18 U.S.C. § 1001, the Standards of Ethical Conduct for Employees of the Executive Branch (5 C.F.R. § 2635.902(v)); and VA Handbook 5025, Legal, Parts III and IV. (April 15, 2002).

[27] 44 U.S.C. §§ 2911, 3301.

Conclusion

The OIG found that on multiple occasions in September and October 2016, the OIT program manager and the VHA employee falsely represented to the approving official, the VA's approving official for the CRADA, that the proposed CRADA with Flow Health was ready for his approval and signature. Moreover, they concealed material information pertaining to significant unresolved concerns raised by VA privacy experts. With the Department of Justice's declination for prosecution, the OIG makes the following recommendations to VA regarding potential administrative actions. Relevant VA management officials concurred with both recommendations. Management's full response is printed as appendix C.

Recommendations

1. The Assistant Secretary for Information and Technology and Chief Information Officer confers with the Office of General Counsel and the Office of Human Resources and Administration/Operations, Security, and Preparedness to determine, given the facts and circumstances, whether any administrative action should be taken with respect to the OIT program manager's conduct.
2. The Executive in Charge, Veterans Health Administration, confers with the Office of General Counsel and the Office of Human Resources and Administration/Operations, Security, and Preparedness to determine, given the facts and circumstances, whether any administrative action should be taken with respect to the VHA employee's conduct.

Appendix A: Scope and Methodology

The OIG reviewed applicable laws, regulations, policies, and guidelines. The OIG interviewed the OIT program manager, the VHA employee, the approving official, the VHA chief health technology officer, and the deputy chief counsel of the OGC Health Care Law Group. In addition, the OIG reviewed transcripts of sworn testimony of VA employees obtained by the former VA Office of Accountability Review during an administrative investigation board of inquiry into the Flow Health CRADA. The OIG issued 22 subpoenas and collected and reviewed financial records, emails of relevant VA staff, telephone and text messaging records, and other documentation received from OGC, OIT, and VHA staff in response to document requests.

In this report, the OIG has generalized narratives and case scenarios and has removed identifiers for individuals when appropriate to protect the privacy and identity of parties and witnesses.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Investigations.*

Appendix B: False Statements and Concealment of Material Facts

As detailed below, in the weeks leading up to the execution of the CRADA on October 28, 2016, the OIT program manager and the VHA employee made multiple false statements to the approving official as they advocated that he execute the CRADA. For context, the chronology also includes related communications between the OIT program manager or the VHA employee and the Flow Health CEO.

False Statements on September 27, 2016

Sept. 27 7:01 p.m.	While on the telephone with the Flow Health CEO, the OIT program manager emailed the approving official (with the VHA employee on copy), saying, Today we provided the responses to your review questions for the proposed final approval of the Flow Health "Medical Knowledge Graphs" CRADA Project. Attached please find the responses and the attached signature-ready CRADA project document. We appreciate it if we can review the responses and approve tomorrow September 28. Let us know if you have any questions. Attached to this email was a document dated September 27, 2016, titled, *Flow Health Medical Knowledge Graphs Project Review Responses for CRADA Approval.* In the document, the OIT program manager presented the following question and answer to the approving official: 1. **Question:** Cybersecurity implications involving access to Web services, electronic messaging between providers and veterans, including store-and-forward, telehealth messages, etc. and Individually Identifiable Information (PHI and PII) – Technical Transfer statement on pages 17-18 of the proposal. **Response**: **The CRADA project proposal, patient data access and privacy implications, were [r]eviewed and approved by both VA OIS and OGC**. [Emphasis added.] This confirms the protection of patient data privacy and cybersecurity according to the CRADA document: • VA and Flow Health will sign a Business Associate Agreement (BAA) prior to Flow Health getting data or systems access. (Reference: CRADA document page 19 Milestones, Phase 1 Data Access.) • In accordance with the CRADA document and BAA, Flow Health will de-identify data before conducting research. (Reference: CRADA document page 15–16 Research Approach, de-identifying for research.)

	• Flow Health currently operates under FISMA Moderate within Amazon Web Services. Flow Health will use the FISMA High AWS GovCloud as required by VA.

OIG Analysis

The OIT program manager's statement to the approving official that the OIS had reviewed and approved the CRADA proposal for "privacy implications" was false because OIS's ISO did not review it for privacy issues.

The OIT program manager's statement to the approving official that the OGC had reviewed and approved the CRADA proposal for "privacy implications" was false because the OGC deputy chief counsel's approval of the CRADA on September 15, 2016, was premised on the OIT program manager's misrepresentation to her that VHA privacy officials were comfortable with the CRADA. The VHA privacy officer did not become aware of the proposed CRADA with Flow Health until early October 2016. Moreover, upon learning of the proposed CRADA in early October, the VHA privacy officer raised significant concerns that were not fully addressed by the OIT program manager or the VHA employee.

Concealment of Material Facts on October 6, 2016

Oct. 3, 6:20 p.m.	The OIT program manager emailed the ISO a copy of the proposed CRADA and BAA document and asked her to review and approve the BAA document. In his email to the ISO, the OIT program manager said, "As we move through review/approval please can you read and concur with the attached BAA including comments on security and privacy assurance and provide back tomorrow October 4."
Oct. 4, 1:28 p.m.	The OIT program manager emailed the executive director of OIT Enterprise Cybersecurity Strategy (the executive director) (copying the approving official and the VHA employee) a copy of the proposed CRADA: Good meeting you here. [the approving official] referenced our OI&T CRADA Project, Flow Health Medical Knowledge Graphs. Through this development that we are collaborating, we aim to learn and discover how this platform uses analytics that will better inform clinicians and patients with advanced accuracy and personalized … diagnostic information. This is to ask if you might have any suggested comment in relation to privacy. We are using the Business Associate Agreement with our collaborator. Please if you can let us know any thought by tomorrow COB Wednesday October 5th that would be helpful with our final review/approval.
9:00 p.m.	The OIT program manager placed an 11-minute call to the Flow Health CEO.
Oct. 5, 7:36 a.m.	Replying to the OIT program manager's request on October 3 that she review and approve the BAA, the ISO emailed the OIT program manager, the VHA employee and the Flow Health CEO, and said, "The BAA looks good **but please include verbiage regarding VA preserving it's [sic] right to conduct random and/or routine HIPAA Privacy, Security and Breach Notification audits.**" (Emphasis added.)
9:35 a.m.	The Flow Health CEO replied to the ISO (with the OIT program manager and the VHA employee on copy) and provided alternate language regarding VA preserving it's [sic]

	right to conduct random and/or routine HIPAA Privacy, Security and Breach Notification audits.[28]
10:40 a.m.	In a different email discussion pertaining to the OIT program manager's request to the executive director on October 4, at 1:28 p.m. (above), the executive director replied to the OIT program manager (with the approving official and the VHA employee on copy), saying, "For privacy, I would recommend you connect with our Privacy Office, headed by [the OIT privacy official]. He is copied on this message and can connect you with the right people to review what you sent."
11:09 a.m.	Returning to the separate email discussion pertaining to the OIT program manager's request for the ISO to review and approve the BAA, the ISO replied to the OIT program manager, the VHA employee and Flow Health CEO, saying, "Ok, the 30 days as reasonable notification **may not suffice or there may need to be more elaborate verbiage on this**. I am checking on that current standard." (Emphasis added)
11:14 a.m.	The ISO emailed the OIT program manager, the VHA employee and the Flow Health CEO again and advised them, "**Let's move forward with submission of BAA to [the deputy chief counsel] for OGC review and approval. The BAA looks fine other than that concern I had but I will research the current standard and any further verbiage that may needed [sic] to appropriately address auditing, specifically in regards to data breach notification/prevention protocol.**" (Emphasis added)
11:21 a.m.	The OIT program manager emailed a copy of the BAA to the deputy chief counsel (with the approving official, the VHA employee, the Flow Health CEO and the ISO on copy). The OIT program manager wrote, "FYI sharing with you a copy of the draft BAA we have for Flow Health."[29] (Emphasis added.)
11:55 a.m.	Responding to the executive director's email from October 5, 2016 at 10:40 a.m. (above), the OIT privacy official replied to the OIT program manager (with the executive director, the approving official, the VHA employee, and two staff from his privacy team on copy), saying, "I would like the Privacy team to have a look at this – we are currently in a tussle with [another federal agency] regarding privacy related to the Million Veteran Program and rather than deal with any potential aftermath I would like to head off any issues before they occur."
Oct. 6, 11:07 a.m.	While on the phone with the Flow Health CEO, the OIT program manager forwarded the OIT privacy official's email from October 5, 2016, at 11:55 a.m., to the Flow Health CEO.
11:38 a.m.	The OIT program manager removed the approving official from the email thread and replied to the OIT privacy official, saying, Thanks for your feedback and interest. In this particular collaboration, we have worked with our OGC and OIS to put together a Business Associate Agreement (BAA) that enforces the HIPAA Privacy Rule on all PHI/PII.

[28] In his reply, the Flow Health CEO stated, "We added the following audit rights language in Sec. 2.11: '[Business Associate agrees that it shall]. Make available to Covered Entity within thirty (30) days of Covered Entity's written request, during normal business hours, all facilities, systems, records, books, agreements, policies and procedures relating to the use and/or disclosure of Covered Entity's PHI for purposes of enabling Covered Entity to determine Business Associate's compliance with the HIPAA Regulations.'" (Brackets in original.)

[29] In his email, the OIT program manager did not request the deputy chief counsel to "review and approve" the BAA, as the ISO had instructed.

	As such the collaborator has much stricter compliance obligations than a traditional research partner. With that said I think we have the necessary requirements in place to move forward. We hope this added information helps clarify. We thank you for your support. Please let [sic] know if you have any questions today. The OIT program manager forwarded this message to the Flow Health CEO at 11:38 p.m.
11:47 a.m.	The OIT privacy official emailed his concerns with the proposed CRADA to the OIT program manager and the VHA employee, stating, [OIT program manager] – I appreciate [sic] opportunity to look this over and comment. Below are the observations of our team and some of the areas of concern they raised. In addition to our folks, I've included VHA's Privacy Officer.. for her awareness. Its [sic] been my experience in working with [the Million Veteran Program (MVP)], that efforts involving research present unique challenges that require additional scrutiny. I would much rather err on the side of caution when dealing with PII/PHI. That being said, we are available, as I'm sure VHA Privacy is, to work with anybody to address the issues we've raised. 1. Due to ongoing access to eHMP database and transfer of voluminous PII/PHI, [sic] need Privacy staff dedicated to this project to assure Privacy oversight (similar to Research Privacy Officer). 2. SOW [statement of work] did not mention any Privacy & Security training for Collaborator staff who will have access to VA PII/PHI. 3. This BAA is between VHA and Flow Health and as such it is recommended that they use the compliant approved (by OGC and VHA Health Information Access Office) VHA BAA template. It appears as though this document doesn't conform to the current template posted on VHA's Data Portal listed here (and attached for others to review/confirm). [hyperlink removed] 4. During a cursory comparison of the Flow Health vs. the National BAA template there are some areas that are inconsistent (almost less restrictive to some extent)…i.e. incident/breach notification, termination clause). 5. Overall recommendation is contact BAA [name and phone number redacted] to ensure Flow Health BAA is consistent and meets National BAA requirements. The OIT program manager forwarded this message to the Flow Health CEO at 11:47 a.m.
3:23 p.m.	The OIT program manager obtained the "National [VHA] BAA template" that the OIT privacy official had referenced in his 11:47 a.m. email above (item 4), and sent the VHA BAA document to the Flow Health CEO and the VHA employee.

4:50 p.m.	The Flow Health CEO emailed the VHA BAA, signed by him, to the OIT program manager and the VHA employee.
5:57 p.m.	While on the telephone with the Flow Health CEO, the OIT program manager sent an email to the approving official, (with the VHA employee on copy), telling the approving official, Attached for your review/signature you will find the Flow Health Medical Knowledge Graphs CRADA (9/28/16). Also, attached is the VHA BAA National standard form signed by Flow Health for your information. This will be signed by [the VHA employee]. **We completed the necessary reviews per our conversations and the CRADA is ready for your signature**. (Emphasis added.)

OIG Analysis

The OIT program manager's statement at 5:57 p.m., "We completed the necessary reviews per our conversations and the CRADA is ready for your signature." was a concealment of a material fact from the approving official because, when the OIT program manager sent this email, the OIT program manager knew that earlier that same day, the OIT privacy official had relayed to him (and to the VHA employee) several significant concerns regarding the proposed CRADA that had not been communicated to the approving official and had not been fully addressed.

False Statement on October 11, 2016

Oct. 11, 4:22 p.m.	While on the telephone with the Flow Health CEO or immediately thereafter, the OIT program manager sent another email to the approving official, (with the VHA employee on copy), telling him, This is the Flow Health proposed CRADA, for your approval and signature. **We completed a review and have concurrence on privacy and security.** The BAA for privacy assurance is attached too. As we mentioned if you can review and sign electronically here that would be great. (Emphasis added.)

OIG Analysis

This statement was false because at the time the OIT program manager sent this email to the approving official, there was no concurrence by privacy and security officials. To the contrary, the OIT privacy official raised several privacy concerns that had not been fully addressed. The OIT program manager's statement to the approving official that they had concurrence on "security" was false because the ISO did not review the CRADA. In addition, these concerns had not otherwise been communicated to the approving official.

Concealment of Material Facts on October 14, 2016

Oct.12, 3:19 p.m.	The VHA privacy officer emailed concerns with the proposed CRADA to the OIT program manager and the VHA employee, telling them, I have various privacy concerns, but I am also concerned about the CRADR [sic] and how it has been executed. I am adding [the regulatory affairs official] to this message as she handles regulatory affairs for research and compliance with the Common Rule for ORD to address any questions with the CRADA. As for the Business Associate Agreement (BAA), we do not do BAAs for research activities as directed by HHS OCR who enforces the HIPAA Regulations. Authority to use and disclose protected health information (PHI) for research purposes is the IRB-approved or Privacy Board-approved waiver of HIPAA Authorization or a signed, written authorization from the study subject. For information purposes the HIPAA Privacy Rule at 45 CFR 164.501 defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." Any activity using VHA PHI that meets this definition is research regardless of whether it is human subjects research or not.
4:47 p.m.	The regulatory affairs official identified concerns with the CRADA in an email to the OIT program manager and the VHA employee, telling them, I have just begun reviewing the emails and glancing thru the CRADA, but I have some human subject protection issues that need to be addressed based upon the SOW, including access to MVP health data by an external Collaborator based upon MVP's informed consent language. The SOW is not the protocol, so I would like to request access to the protocol so that I can ascertain VA's role is [sic] this protocol vs. the collaborators. However, a key issue I would like to query initially concerns VA's conduct of the proposed research activity. VHA is the only component that has been given the authority within the Agency to conduct research. Regardless of whether or not this is human subjects research subject to IRB review and approval, human subjects research exempt from IRB review and approval, or non-human subjects research, VA Research and Development Committee approval is required in addition to the applicable subcommittees. Do all VA OI&T employees involved in the conduct of this proposed research activity have an appointment (e.g., WOC) at a VA Facility that can conduct research? Also, who is the OGC Specialty Team Advisory Research attorney who reviewed this CRADA?[30]
Oct. 13, 10:11 a.m.	The OIT program manager placed a four-minute call to the Flow Health CEO.

[30] Alarmed by the CRADA's commitment of research data from the MVP, the regulatory affairs official contacted the MVP team and asked if they knew that the CRADA obligated the release of MVP program research data to Flow Health. The answer was no. The regulatory affairs official followed up her email with a telephone call to the OIT program manager. He did not answer so the regulatory affairs official left him a voice message telling him that he could not use MVP data and asked him to call her back.

10:36 a.m.	The Flow Health CEO sent an email to the approving official (with the OIT program manager and the VHA employee on copy), saying, "Thank you again for your support on our collaboration. I look forward to receiving your final approval and signature on the CRADA. We are excited and eager to begin our work on this initiative."
Oct. 14, 9:34 a.m.	The OIT program manager placed an 18-minute call to the Flow Health CEO.
10:36 a.m.	The OIT program manager sent an email to the approving official (with the VHA employee on copy), stating, "Reminder: Unless any more questions, would you be able to electronically sign Flow Health CRADA? We provided the bundled package to you, CRADA SOW with the national Business Associates Agreement?"
10:40 a.m.	While on the telephone with the Flow Health CEO, the OIT program manager forwarded the VHA privacy officer's email from October 12, 2016, to the Flow Health CEO.

OIG Analysis

The OIT program manager's October 14, 10:36 a.m. email concealed material facts because, at the time the OIT program manager sent it to the approving official, the OIT program manager knew that the OIT privacy official, the VHA privacy officer, and the regulatory affairs official had relayed to him (and to the VHA employee) several significant concerns regarding the proposed CRADA that had not been communicated to the approving official and had not been fully addressed.

Concealment of Material Facts and False Statements on October 17, 2016

Oct. 17, 9:13 a.m.	The OIT program manager emailed the approving official (with the VHA employee and the Flow Health CEO on copy), stating, "[Approving official,] Reminder for today. If there aren't additional questions we should be ready to sign attached CRADA and BAA concurred. If you might like, [the VHA employee] and Flow Health CEO are available to meet as well today. You may decide to sign the CRADA electronically here, please let us know."
2:27 p.m.	The approving official replied to the OIT program manager's email (with the VHA employee, the Flow Health CEO, and the approving official's executive assistant on copy), saying, I have reviewed the 2 documents. My questions: 1. Who will give the vendor [Flow Health] access to eHMP? 2. Who will sign the BAA for VA? **3. Has OIS reviewed the CRADA and BAA?** (Emphasis added.)
2:29 p.m.	The Flow Health CEO placed a two-minute-and-34-second call to the VHA employee.
2:48 p.m.	The VHA employee replied to the approving official answering his questions, stating, 1. Flow Health already has access to the eHMP sandbox. The VistA Evolution Program team will be providing production access to Flow

	Health. We will be working in partnership with OIS to support this process. 2. The BAA is between VHA and Flow Health. As such, [the VHA chief health technology officer] can sign the BAA on behalf of VHA once we have a signed CRADA that establishes the documented relationship.[31] **3. Yes. OIS has reviewed and approved both the CRADA and the BAA.** (Emphasis added.)
2:53 p.m.	The approving official replied to the VHA employee's answers from 2:48 p.m. by interspersing additional questions, as follows: 1... Is this documented in the CRADA? I did not see this. 2… Great. Please remind me, does the CRADA specifically point to the BAA as a requirement? **3... Who? Documented? Signature on something?** (Emphasis added.)
2:56 p.m.	The Flow Health CEO placed a four-minute call tothe VHA employee.
2:58 p.m.	While on the telephone with the Flow Health CEO, the VHA employee replied to the approving official (copying the OIT program manager and Flow Health CEO), saying, 1. Yes – Milestones phase 1 data access 2. Yes – Milestones Phase 1 data access **3. [Information security officer] – CC'd if she has comment but I've attached the extracted emails.** (Emphasis added.)
3:26 p.m.	The approving official replied to the VHA employee (with the OIT program manager, the Flow Health CEO and the ISO on copy), and said, "[VHA employee], 1 & 2: not clear to me in CRADA. 3. Did we make the edits requested?"

OIG Analysis

The OIT program manager's 9:13 a.m. email concealed material facts because, when the OIT program manager sent it to the approving official, the OIT program manager knew that the OIT privacy official, the VHA privacy officer, and the regulatory affairs official had relayed to him (and to the VHA employee) several significant concerns regarding the proposed CRADA that had not been communicated to the approving official and had not been fully addressed.

The VHA employee's 2:48 p.m. response to the approving official's third question, in which he stated, "Yes. OIS has reviewed and approved both the CRADA and the BAA," was false. First, the statement that the CRADA was approved by "OIS" was false because the ISO never approved the CRADA. Second, the statement that the BAA was approved by "OIS" was false because the ISO did not review and approve the VHA BAA until October 19, 2016.

The VHA employee's statement at 2:58 p.m. was a continuation of his false statement at 2:48 p.m. Specifically, in answering the approving official's third question in this email, the VHA employee provided the name of the ISO who he represented had reviewed and approved the

[31] The VHA chief health technology officer told the OIG that he never had the authority to sign a Business Associate Agreement on behalf of the VHA and never discussed signing one with anyone.

CRADA and the BAA. As explained above, the statement that the CRADA was approved by "OIS" was false because the ISO never approved the CRADA. Second, the statement that the BAA was approved by "OIS" was false because the ISO did not review and approve it until October 19, 2016.

Misleading Statement to Approving Official on October 19, 2016

Oct. 17, 4:46 p.m.	While on the phone with the Flow Health CEO, the OIT program manager sent the VHA BAA document, signed by the Flow Health CEO, to the ISO and asked her to "confirm that the VHA BAA meets OIS approval for the Flow Health CRADA including all HIPAA, privacy, security and breach notification audit requirements."
5:04 p.m.	The Flow Health CEO placed a call to the VHA employee and added him to the call with the OIT program manager. The three-way call lasted eight minutes.
Oct. 19 8:57 a.m.	Responding to the OIT program manager's request from October 17 at 4:46 p.m. to "confirm that the VHA BAA meets OIS approval for the Flow Health CRADA including all HIPAA, privacy, security and breach notification audit requirements[,]" the ISO replied to the OIT program manager, the VHA employee and the Flow Health CEO and said, Yes, that official OGC guidance and approval regarding use of VHA BAA Template will meet these BAA verbiage requirements outlining HIPAA, Privacy, Security, VA Breach Notification/Prevention and Audit Procedures/Requirements. I have no further concerns with the OGC approved BAA meeting these requirements.
1:55 p.m.	The Flow Health CEO placed a 13-minute call to the VHA employee.
2:14 p.m.	The Flow Health CEO placed a 28-minute-and-31 second call to the OIT program manager.
2:42 p.m.	While on the telephone with the Flow Health CEO, the OIT program manager sent an email to the approving official (with the VHA employee and the Flow Health CEO on copy), stating, "**We have approval from Privacy, Security and Legal.** Attached is the updated CRADA signed by our Collaborator ([Flow Health CEO]), [the VHA employee] and myself. **It is my recommendation that we move forward and finalize the CRADA with your signature.**" (Emphasis added.)
5:59 p.m.	The VHA employee forwarded the OIT program manager's 2:42 p.m. email to the approving official, telling him, "I agree with [the OIT program manager]'s recommendation."

OIG Analysis

As to the email at 2:42 p.m., the OIT program manager's statement was false because at the time the OIT program manager sent this email to the approving official, there was no approval of the CRADA as it related to privacy. To the contrary, the OIT privacy official, the VHA privacy officer, and the regulatory affairs official had raised a number of significant concerns that had not been fully addressed. In addition, these concerns had never been communicated to the

approving official. Moreover, the OIT program manager's statement to the approving official that they had approval from "Legal" was false because the deputy chief counsel's approval of the CRADA on September 15, 2016, was premised on the OIT program manager's misrepresentation to her that VHA privacy officials were comfortable with the CRADA. The VHA privacy officer did not become aware of the proposed CRADA with Flow Health until early October 2016 and had raised significant concerns that were not fully addressed by the OIT program manager and the VHA employee.

The VHA employee's 5:59 p.m. email was misleading because the VHA employee endorsed the OIT program manager's previous false statement knowing that the OIT privacy official, the VHA privacy officer, and the regulatory affairs official had raised a number of significant concerns that had not been fully addressed. In addition, these concerns had never been communicated to the approving official.

Concealment of Material Facts on October 25, 2016

Oct. 20, 7:33 a.m.	The approving official replied to the OIT program manager's and the VHA employee's emails from the day before, (with the Flow Health CEO on copy), saying, I do not recall suggesting that we change the BAA.[32] I want to make sure: 1. The correct VE staff have agreed to provide the required access; 2. That all cybersecurity requirements have been met. 3. That 1 and 2 are properly (completely) documented (the right signatures). For #2, maybe we should have a quick call with [the ISO].
9:07 a.m.	The Flow Health CEO placed a 30-second call to the OIT program manager.
11:33 a.m.	The OIT program manager placed a 17-minute call to the Flow Health CEO.
Oct. 24, 11:01 a.m.	The Flow Health CEO sent an email to the OIT program manager and the VHA employee, Subject: "Updated CRADA, Signed by [Flow Health CEO]," saying, Attached is a redlined version with the following additions. I've also included a clean Word version and a signed PDF. • P. 19: Data Access. VA will ensure Collaborator has access to VA Health Data through a secure connection to VA systems for data exchange of Protected Health Information (PHI) and Personally Identifiable Information (PII). • P. 22: Learning the process for establishing connectivity between VA systems and a cloud-based platform to exchange PHI/PII in a secure manner. [OIT program manager], I have reviewed the additions with [the VHA employee] and he felt they meet [the approving official]'s expectations.

[32] In his email dated October 6, 2016, at 11:47 a.m., the OIT privacy official told the OIT program manager and the VHA employee of several concerns with the proposed CRADA, which included that they had used an incorrect BAA template. The approving official's statement in his October 20 email that he did not recall suggesting they change the BAA further demonstrates that the OIT program manager and the VHA employee never told the approving official about the OIT privacy official's concerns.

	If you agree, let's sign and circulate to [the approving official] for his signature. Feel free to call me when you have a break."
Oct. 25, 8:38 a.m.	The VHA employee replied to the Flow Health CEO's email from the day before (with the OIT program manager on copy), saying, "Signed by me. [OIT program manager] was this approved by [the approving official] so you can just sign and send along to get his signature?"
11:07 a.m.	The OIT program manager forwarded the VHA employee's email and the proposed CRADA that was signed by the Flow Health CEO and the VHA employee to the approving official, saying, Attached below you will find for your review, the updated Data Access and Learning Process statements, their location in the CRADA document, and the updated document signed by [Flow Health CEO] and [the VHA employee]. Please if you can let us know if this is agreeable for approval, then I can sign prior to your signature tomorrow Wednesday upon return from travel. As well we're available for any follow-ups. I want to [t]hank [Flow Health CEO], [ISO] and [the VHA employee] for their [g]ood [c]ollaborative [w]ork.

OIG Analysis

The OIT program manager's October 25, 11:07 a.m. statement was a concealment of a material fact because, at the time the OIT program manager sent this email to the approving official, the OIT program manager knew that the OIT privacy official, the VHA privacy officer, and the regulatory affairs official had relayed to him (and to the VHA employee) several significant concerns regarding the proposed CRADA that had not been communicated to the approving official and had not been fully addressed.

Concealment of Material Facts on October 27, 2016

Oct. 27, 9:30 a.m.	The OIT program manager sent an email to the approving official (with the VHA employee and the Flow Health CEO on copy) stating, This is the revised proposed final Flow Health CRADA document for your approval/signature. If you agree and would electronically sign the document that would be great. We have included the two statements on the document pages indicated below for your convenience, that cover Data Access and Learning the process for establishing connectivity with PHI/PII under the CRADA. [The VHA employee], [the Flow Health CEO] and I have signed. P. 19: Data Access. VA will ensure Collaborator has access to VA Health Data through a secure connection to VA systems for data exchange of Protected Health Information (PHI) and Personally Identifiable Information (PII). P. 22 under Evaluation Approach: Learning the process for establishing connectivity between VA systems and a cloud-based platform to exchange PHI/PII in a secure manner.

OIG Analysis

The OIT program manager's 9:30 a.m. email conceals a material fact because, at the time the OIT program manager sent this email to the approving official, the OIT program manager knew that the OIT privacy official, the VHA privacy officer, and the regulatory affairs official had relayed to him (and to the VHA employee) several significant concerns regarding the proposed CRADA that had not been communicated to the approving official and had not been fully addressed.

Concealment of Material Facts on October 28, 2016

Oct. 27, 2:15 p.m.	The OIT program manager placed a four-minute call to the Flow Health CEO.
2:39 p.m.	The VHA employee placed a 13-minute call to the Flow Health CEO.
3:52 p.m.	The VHA employee sent an email to the approving official (with the OIT program manager and the Flow Health CEO on copy), stating, "Do you think this represents the changes we discussed well? If so when will you be able to sign? Once we have your signature for the CRADA we can start the paperwork processes for the serial processes as we discussed with [the ISO] to get the BAA signed and other processes to line everything up for work to begin."
Oct. 28, 9:59 a.m.	The approving official signed the CRADA.

OIG Analysis

The VHA employee's 3:52 p.m. message conceales a material fact because, at the time the VHA employee sent this email to the approving official, the VHA employee knew that the OIT privacy official, the VHA privacy officer, and the regulatory affairs official had relayed to the OIT program manager (with him on copy) several significant concerns regarding the proposed CRADA that had not been communicated to the approving official and had not been fully addressed.

Appendix C: Management Comments

Response of the Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer

Department of Veterans Affairs Memorandum

Date: May 15, 2020

From: Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer (005A)

Subj: OIG Draft Report, *False Statements and Concealment of Material Information by VA Information Technology Staff*, (Project No. 2017-01980-IQ-0099)

To: Acting Executive Director, Office of Special Reviews (56)

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, *False Statements and Concealment of Material Information by VA Information Technology Staff* (Project No. 2017-01980-IQ-0099). The Office of Information and Technology submits the attached written comments. For questions related to OIT's comments on the OIG draft report, please contact Martha Orr, Deputy Chief Information Officer for Quality, Performance, and Risk at 202-461-5139, or have a member of your staff contact La Portia Pratt, Director, Office of Compliance Tracking at 202-461-6934.

(Original signed by:)

Dominic Cussatt

Attachment

005 Attachment

Office of Information and Technology
Comments on OIG Draft Report,
False Statements and Concealment of Material Information by VA Information Technology Staff, Project No. 2017-01980-IQ-0099

OIG Recommendation 1: ***The Assistant Secretary for Information and Technology and Chief information Officer conferred with the Office of General Counsel and the Office of Human Resources and Administration / Operations, Security, and Preparedness to determine, given the facts and circumstances, whether any administrative action should be taken with respect to [the OIT program manager]'s conduct.***

OIT Comments: Concur. Review of the draft report and consultation with Human Resources Employee and Labor Relations indicates that administrative action is warranted based on the facts contained in the report. Appropriate action will be recommended consistent with the Table of Penalties for Title 5, Hybrid Title 38 and Title 38 Employees. Final recommendation and concurrence with General Counsel cannot be provided until the final report is received and reviewed.

Target Completion Date: May 31, 2020

Response of the Executive in Charge, Office of the Under Secretary for Health

Department of Veterans Affairs Memorandum

Date: April 17, 2020

From: Executive in Charge, Office of the Under Secretary for Health (10)

Subj: OIG Draft Report, False Statements and Concealment of Material Information by VA Information Technology Staff (VIEWS 02655272)

To: Acting Executive Director, Office of Inspector General, Office of Special Reviews (56)

1. Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, False Statements and Concealment of Material Information by VA Information Technology Staff. I have attached the action plan to address recommendation 2.

2. If you have any questions, please email Karen Rasmussen, M.D., Director for GAO-OIG Accountability Liaison at VHA10EGGOALAction@va.gov.

(Original signed by:)

Richard A. Stone, M.D.

Attachment

VETERANS HEALTH ADMINISTRATION (VHA)
Action Plan

OIG Draft Report: False Statements and Concealment of Material Information by VA Information Technology Staff

Date of Draft Report: April 7, 2020

Recommendations/ Actions	Status	Target Completion Date

Recommendation 2: The Executive in Charge, Veterans Health Administration, confers with the Office of General Counsel and the Office of Human Resources and Administration/Operations, Security, and Preparedness to determine, given the facts and circumstances, whether any administrative action should be taken with respect to [the VHA employee]'s conduct.

VHA Comments:

The Veterans Health Administration Office of Health Informatics will confer with the Office of General Counsel and the Office of Human Resources and Administration/Operations, Security, and Preparedness or other appropriate offices to determine whether administrative action should be taken with respect to [the VHA employee]'s conduct.

Status: In progress Target Completion Date: 90 days after receipt of evidence

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Primary Contributors	Charles Millard, Senior Administrative Investigator Silvia Gonzalez Roman, Supervisory Investigative Attorney
Other Acknowledgments	Domingo Alvarez, Senior Administrative Investigator Sabrina Gregory, Auditor Dyanne Griffith, Attorney Advisor Michele Hale, Administrative Investigator Clifford Stoddard, Attorney Advisor Leanne Watkins, Senior Administrative Investigator

Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Assistant Secretaries
General Counsel

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget