DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration
Silver Spring, MD 20993

JUL 13 2012

The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510-6275

Dear Senator Grassley:

Thank you for your letter of January 31, 2012, requesting information about the use of computer monitoring by the Food and Drug Administration (FDA or the Agency) to investigate the illegal and unauthorized release of confidential information related to medical device applications and submissions.

In connection with this matter, there are several cases in active litigation and open investigations by the U.S. Office of Special Counsel (OSC). Further, on June 14, 2012, in response to a request from OSC, the Secretary of Health and Human Services (HHS) asked the HHS Office of Inspector General (OIG) to conduct an investigation of the premarket review process for some medical device applications and submissions, which, in part, relate to the aforementioned unauthorized disclosures. The litigation, OSC investigations, OIG referral, and commensurate need to understand all the facts surrounding the improper disclosure of confidential information, and the subsequent Agency response, require a thorough and deliberate review of events. This review must respect the rights of individual employees as well as protect governmental legal prerogatives. Such constraints might limit the Agency's response to questions related to matters involved in the litigation and open investigations. Please accept my apology for the delay in responding due to the pending investigations and litigation related to this matter.

FDA recognizes and appreciates your interest in the issues raised in your letter. We share your concern that our employees be afforded all appropriate and available opportunities to raise issues relating to Agency policies and decisions. At the same time, FDA has important obligations to ensure the integrity of the medical device premarket review process, which requires FDA, including the Center for Devices and Radiological Health (CDRH), to routinely receive and review trade secrets and confidential commercial information submitted by regulated entities, the disclosure of which could cause competitive harm to the company submitting the information. Congress has enacted statutes that expressly prohibit FDA personnel from disclosing trade secrets and confidential commercial information. Such unauthorized disclosures not only violate federal law and undermine the integrity of FDA programs; they also can result in civil suits against FDA and/or criminal and monetary penalties against its employees. In many instances, the mere fact that a device firm has submitted a premarket submission or application is itself confidential. Similarly, details about a company's product in development, or the data and

information concerning a product's safety and effectiveness, could give the company's competitors an unfair advantage by providing previously unavailable insights into the development process, and disclosure of such details could undermine incentives for innovation and competition in the commercial market. Protection of this highly sensitive information is of utmost importance to FDA.

Please note that this letter reflects FDA's current understanding of the facts pertaining to this inquiry and is based upon the Agency's review of the matter to date.

Your letter characterizes the signatories of a January 2009 letter as the "nine whistleblowers," and it is these individuals to whom we understand your questions generally relate, as well as to Lakshmi Vishnuvajjala, who, though not a signatory, was one of the five individuals whose computer activity was monitored by FDA pursuant to the Agency's investigation into suspected unauthorized disclosures by CDRH personnel.

We have restated your questions below in bold, followed by our responses.

1. **Who authorized the monitoring of all of the whistleblowers email accounts for communications with Congress?**

The question of the authorization of monitoring is being addressed in the OSC investigation that you and Chairman Issa have requested, as well as the pending litigation, and the Agency is still identifying and gathering evidence with respect to these issues.

2. **Are any of the original nine FDA physicians and scientists that wrote the letter to the Presidential Transition Team in 2009 still employed by FDA? If not, please provide the circumstances surrounding each of their departures.**

Five of the nine individuals to whom you refer continue to be employed by FDA. In addition, Lakshmi Vishnuvajjala, who was one of the five individuals whose computer activity was subject to monitoring, remains employed by FDA.

- Ewa Czerska was a General Schedule employee who was removed from her position on April 29, 2011, for unauthorized disclosure of confidential information. Pursuant to an agreement recently reached between the Office of the Special Counsel and both HHS and FDA, Dr. Czerska has been temporarily reappointed with pay through July 31, 2012.

- Paul Hardy was a Commissioned Corps officer within the U.S. Public Health Service, who was not recommended for promotion by the Annual Promotion Board in September 2011. On October 9, 2011, he was terminated from the Regular Corps pursuant to 42 U.S.C. § 211(g).

- Robert Smith was a Schedule A Appointment Medical Officer. His term appointment expired on July 31, 2010.

- Another individual was at FDA as a limited-term staff fellow appointed pursuant to 42 U.S.C. § 209(g).[1] This person's term appointment expired on November 6, 2010.

3. Did the FDA monitor all employee email accounts, including personal accounts, or was the monitoring targeted only at the nine whistleblowers?

In 2009 and 2010, FDA became aware of a series of unauthorized disclosures of confidential information contained in various medical device premarket applications and submissions under review. For instance, on January 13, 2009, *The New York Times* (*Times*) published an article that included confidential information from iCAD's then-pending premarket approval application (PMA) for its SecondLook Digital Computer-aided Detection for Mammography device. According to information iCAD provided to FDA, the article's author informed the company that he had received "internal FDA documents" regarding the device from "Scientific Officers of the FDA." On January 13, 2009, legal counsel for iCAD sent a letter to the CDRH Ombudsman expressing concern regarding the apparent disclosure by FDA of the company's confidential PMA information. The January 13, 2009, *Times* article also quoted from an internal Agency memorandum regarding the pending review of another firm's premarket submission. A consultation review memorandum on the premarket notification submission (referred to as a "510(k)") had been written on March 14, 2008, by other CDRH personnel to, among others, Dr. Robert Smith, an FDA medical officer.

Then, on April 16, 2010, CDRH received a letter from legal counsel for GE Healthcare Inc., alleging that FDA had disclosed to the press confidential information from one of the firm's premarket notification submissions. The letter referenced a March 28, 2010, *Times* article as evidence that confidential information from the company's 510(k) submission had been leaked to the press in violation of federal law, FDA regulations, and internal Agency policy. This article referred to "[s]cores of internal agency documents made available to The New York Times." Although the article did not disclose the source of the internal agency documents, it included quotes from both Dr. Robert Smith and former FDA contractor, Dr. Julian Nicholas. The firm requested that FDA "conduct an internal investigation into how this information was leaked to the press."

Software-enabling computer monitoring was installed on Dr. Smith's government-issued computer on April 22, 2010—five days after FDA received the GE Healthcare letter alleging unlawful public disclosure of confidential information. During the course of monitoring Dr. Smith's use of his government-issued computer, evidence was uncovered suggesting that certain additional CDRH personnel were participating in unauthorized disclosures of information, and monitoring was expanded to include these additional personnel, as noted below.

- Paul Hardy – May 24, 2010
- Ewa Czerska – June 30, 2010
- Lakshmi Vishnuvajjala – June 30, 2010

---

[1]Due to privacy concerns, we are unable at this time to provide the name of this individual.

- The CDRH staff fellow referenced in FDA's response to Question 2 above – June 30, 2010

As noted below, FDA employees are subject to monitoring of their use of government-owned equipment in accordance with policies developed to comply with the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. 107-347, codified at 44 U.S.C. §§ 3541-3549 (2011)). In fact, since 2009, all users of the FDA computer network have received notice upon logging into an FDA computer that they should have no reasonable expectation of privacy when utilizing the FDA computer system.[2]

Monitoring in this case occurred only with respect to the five individuals identified above. FDA did not monitor the individuals' use of non-government-owned computers at any time. To the extent FDA personnel elected to use a government computer to engage in correspondence using a personal e-mail account, data derived from such use would have been collected in the same manner as any other of his or her uses of the government-issued computer.

Finally, FDA wishes to take this opportunity to address your concern that FDA initiated the computer monitoring described herein upon learning that the individuals were communicating with Congress.[3] Beginning as early as October 2008, FDA had begun receiving letters and other inquires from multiple Congressional offices regarding concerns brought to them by various members of the group of individuals you reference. These inquiries made clear that CDRH personnel were seeking the intervention of Congress. Nonetheless, it was not until approximately 18 months after FDA began to receive such inquiries that the monitoring of Dr. Smith's government-owned computer activity was initiated. The impetus for the monitoring was not any communication to Congress. Rather, the impetus for monitoring was the March 2010

---

[2] For example, upon logging on to the FDA network, users immediately receive the following warning message:

> You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.
>
> This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
>
> By using this information, you understand and consent to the following:
>
> - You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
> - Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

The above warning has been in continuous use since at least September 2010, and a similar warning was in use at the time the monitoring, as described herein, was initiated. Additionally, all FDA personnel are required to receive Computer Security Awareness Training annually, during which they are reminded, among other things, that all network activity may be monitored. The employees about whom you have inquired received such annual training.

[3] *See* 158 Cong. Rec. S3468 (daily ed. May 23, 2012) (statement of Sen. Grassley).

Times article and the receipt of the GE Healthcare letter just prior to the initiation of monitoring, which indicated that the preceding pattern of similar unauthorized disclosures of confidential information from other pending medical device applications and submissions was continuing unabated. It should also be noted that, in conducting the computer monitoring, data were collected without regard to the identity of the individuals with whom the user may have been corresponding.

FDA initiated monitoring of the government-owned computers of the five individuals identified above for two principal purposes: 1) to identify the source of the unauthorized disclosures, if possible; and 2) to identify any further such unauthorized disclosures so as to better enable FDA to facilitate their cessation.

4. Did FDA obtain the passwords to the employees' personal email accounts, which would allow e-mails to be intercepted even when not sent or received from a government computer?

As noted above, FDA collected data regarding certain personnel's use of their government-owned computers. For each of the individuals subject to computer monitoring, data were collected from the following sources:

- Screenshots, taken every five seconds, of the totality of whatever was visible on one or more monitors in use for a given government-issued computer;
- All e-mail sent or received to/from a given government-issued computer;
- All network activity to/from the government-issued computer;
- All data stored on and printed from the government-issued computer or an external storage drive connected thereto; and
- All keystrokes performed on the government-issued computer.

According to individuals involved at the time, as well as our review of the matter to date, in reviewing the data collected during the course of the computer monitoring, FDA endeavored to identify e-mails being sent to individuals outside the FDA network that appeared to include confidential Agency records, including, in particular, confidential records relating to premarket medical device applications and submissions.

FDA is not aware of any information that suggests that Agency personnel collected passwords for individuals' personal e-mail accounts. According to the forensic engineer principally involved in the computer monitoring, to the extent individuals' passwords may have been captured, it would have been incidental to the objective of the monitoring and FDA did not utilize or otherwise take any action related to such passwords.

To the extent FDA became aware of the use of personal e-mail accounts to transmit information, it was either through the identification of screenshots, which in many cases recorded correspondence that had been accessed on an FDA computer, or because the individual used his or her FDA e-mail account to send Agency records to his or her own personal e-mail address. It

should be noted that once monitored individuals transmitted Agency records to their own personal e-mail account, in many cases the records were almost immediately forwarded further to individuals outside the government.

5. Is FDA currently monitoring any employee email accounts? If so, please provide the circumstances surrounding the monitoring.

FDA is not currently monitoring the e-mail accounts of any of the Agency personnel about whom you have inquired.

When appropriate, FDA may monitor an employee's FDA e-mail account in support of authorized personnel investigations, including, for example, when directed by law enforcement or the Department of Homeland Security. In accordance with FISMA, FDA also employs information technology (IT) security controls throughout the FDA IT Enterprise. These IT controls are employed to ensure the confidentiality, integrity, and availability of FDA data and are consistent with the management, operational, and technical controls outlined in NIST Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations." These IT controls broadly include logging of all system events, monitoring of data entering and leaving the FDA IT Enterprise, and ensuring authorized access to systems. The security controls are further employed to support the protection of intellectual property entrusted to FDA from theft or sabotage.

6. What steps have you taken to reassure employees that they have a right to have direct communications with Congress?

In February 2009, then-acting Commissioner Dr. Frank Torti issued an Agency-wide memorandum detailing whistleblower protections. On January 8, 2010, Commissioner Dr. Margaret Hamburg issued a memo to all FDA employees affirming the Agency's strong support for the Whistleblower Protection Act of 1989 (Pub. L. 101-12, codified at 5 U.S.C. § 2302 (2011)). In the memo, she reminded employees of OSC's complaint management process to address complaints of whistleblower retaliation, and stated that "[r]eprisal against individuals will not be tolerated for disclosure of information in which the employee believes there is reasonable evidence of violation of any law, rule or regulation; ... or a substantial and specific danger to public health or safety." She directed employees to an online training course and provided OSC's web address and phone number.

Under the Notification and Federal Employee Antidiscrimination and Retaliation (NO FEAR) Act of 2002, Pub. L. 107-174, codified at 5 U.S.C. § 2301 note (2011), employees are required to undergo training every two years on their rights and protections. FDA offers an online training course to all new hires and current employees.

7. Does FDA have any procedures to ensure that Congressional correspondence remains confidential?

Federal agencies, including FDA, received two memoranda, dated June 20, 2012, from the Office of Management and Budget and the Office of Special Counsel, relating to legal restrictions and guidelines for the monitoring of employee communications, including electronic mail. In accordance with those memos, FDA is currently reviewing and evaluating its policies and practices to ensure that they are consistent with the law and Congress's intent to provide a secure channel for protected disclosures.

8. Please produce copies of all emails that were intercepted to or from my office by FDA.

FDA is continuing to gather responsive documents.

9. To whom did the Agency give access to any email correspondence to or from Congress, and why?

FDA will respond to this question in a separate response.

10. Please provide all records relating to communications between FDA and iCAD Inc. with respect to the release of confidential business information.

Responsive documents are enclosed. FDA is continuing to search for further responsive documents, which, if identified, will be included in a further response.

Thank you, again, for contacting us concerning this matter. If you have further questions, please let us know.

Sincerely,

Jeanne Ireland
Assistant Commissioner
for Legislation

Enclosures