



DEPARTMENT OF HEALTH & HUMAN SERVICES

05/09/2016  
FDA (HHS)  
Slobodin

Food and Drug Administration  
Silver Spring, MD 20993

The Honorable Fred Upton  
Chairman  
Committee on Energy and Commerce  
House of Representatives  
Washington, D.C. 20515-6115

**MAY 06 2016**

Dear Chairman Upton:

Thank you for your letter of February 17, 2016, cosigned by Chairman Joseph R. Pitts, regarding the Food and Drug Administration's (FDA or the Agency) procedures to protect the trade secret and confidential commercial information (CCI) of regulated entities in the food industry. Please be assured that FDA takes very seriously its responsibility to safeguard trade secret and CCI of regulated industries.

At an FDA-wide level, FDA's Office of Information Management and Technology (OIMT) helps ensure security controls are appropriately applied to FDA systems for the protection of privacy, and helps ensure the confidentiality, integrity, and availability of information stored on FDA's network. One of the highest priorities for OIMT is information protection. Since 2014, OIMT has taken a number of actions to ensure the security of information stored on FDA's network. For example, OIMT has implemented monthly performance metrics to capture cybersecurity activities, improved the FDA security authorization process and streamlined information technology (IT) security reviews, developed key initiatives to ensure FDA IT systems and sensitive information are appropriately safeguarded, and increased cybersecurity awareness across the Agency.

The Center for Food Safety and Applied Nutrition (CFSAN), along with other FDA Centers and offices, works closely with OIMT and its information security/cybersecurity representatives to ensure FDA IT systems and sensitive information are appropriately protected by safeguarding against unauthorized disclosure, access, or misuse.

Regarding your concern about access to proprietary information such as recipes and formulas, we would like to clarify that under section 414(d) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), FDA's access to records does not extend to "recipes for food, financial data, pricing data, personnel data, research data, or sales data (other than shipment data regarding sales)."

As you noted, the FDA Food Safety Modernization Act (FSMA) does expand FDA's access to records. This will help the Agency perform its public health mission, especially when FDA becomes aware of situations such as foodborne illness outbreaks, epidemiological evidence which implicates food causing illness or death, product recalls, adverse event reports, or

consumer complaints that meet the criteria in section 414(a) of the FD&C Act. The expanded records access does not change section 414(d) of the FD&C Act.

Overall, for information received and collected from either foreign or domestic firms, FDA personnel will comply with all applicable protections, procedures, and legal requirements that protect against the unauthorized disclosure of non-public information, such as any trade secret or CCI (see, e.g., 21 U.S.C. section 331(j); 18 U.S.C. section 1905, 21 C.F.R. Part 20).

That being said, the Agency is aware of interest from industry about how FDA will handle this information. For example, the Agency received comments on multiple FSMA rulemakings expressing concern about how FDA will ensure trade secrets and CCI are appropriately protected. FDA has heard similar concerns from stakeholders at FSMA public meetings and outreach activities. FDA recognizes the importance of this issue and has worked to reassure the public in responses to comments and during our outreach that we take these concerns seriously. Every major rulemaking that FDA has issued so far under FSMA clarifies that records obtained by FDA under the new rules are subject to the disclosure requirements in 21 Code of Federal Regulations (CFR) Part 20. In addition, FDA personnel with access to information obtained under the FD&C Act, including the new FSMA authorities, are and will continue to be appropriately trained to comply with all applicable protections, procedures, and legal requirements that prohibit the unauthorized disclosure of non-public information, including any trade secret or CCI. Lastly, it is important to note that section 301(j) of the FD&C Act (21 U.S.C. 331(j)) prohibits the disclosure of trade secrets outside of the Department of Health and Human Services (HHS). Violating section 301(j) of the FD&C Act can subject an individual to civil or criminal penalties.

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

**1. The name and title of the official at the FDA’s Center for Food Safety and Applied Nutrition (CFSAN) responsible for overseeing FDA’s procedures to safeguard trade secret and confidential information. Please provide any documents showing how CFSAN is protecting such information, and also describe the efforts undertaken. Please also describe what efforts have been undertaken with FDA district offices to protect food industry trade secrets and other proprietary information. Is FDA aware of any corporate intelligence monitoring of FDA inspections, such as electronic surveillance of Internet transmissions from hotels where FDA inspectors stay during inspections?**

The protection of trade secret and CCI is of the utmost importance to the Agency. CFSAN shares the responsibility to ensure protection of information with the Office of Foods and Veterinary Medicine directorate and ensures compliance through the strict adherence to HHS and Agency cybersecurity policies, procedures, and guidance. CFSAN also has a Freedom of Information Officer who is responsible for handling any Freedom of Information Act (FOIA) requests. When complex or novel questions about disclosure of information arise, CFSAN consults with FDA’s Office of the Chief Counsel and FDA’s Division of Freedom of Information.

All FDA personnel are required to complete annual Computer Security Awareness Training that outlines individual responsibilities for handling trade secret, company confidential, and other related information (see Enclosure 1). In addition, all new users of HHS information resources must read the *Rules of Behavior for Use of HHS Information Resources* and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks (see Enclosure 2). This acknowledgement must be completed annually thereafter to reaffirm the employee's knowledge of, and agreement to adhere to, the Rules of Behavior.

CFSAN and the Office of Regulatory Affairs (ORA) ensure information protection through the implementation and proper configuration of role-based user access to IT systems. User accessibility and roles are reviewed on a semi-annual basis in order to make sure that approvals for information visibility are still valid and required.

Security and protection of physical records, including foreign food inspection reports, is managed through the CFSAN Document Control Center (DCC). This is a controlled access facility that is only accessible to a limited number of FDA staff who are specifically authorized to review this information. Cleared DCC staff maintain a list of authorized users of record collections containing sensitive and proprietary information.

With regard to FDA district offices, domestic inspection reports and other paper format records, which may or may not contain trade secret or CCI, are stored at FDA Field Offices in a document file room or in file cabinets kept under lock and key and are only accessible by FDA personnel with proper identification or access codes.

With regard to FDA activities abroad, the Agency has implemented a program to provide mobile equipment for overseas travelers to designated countries to reduce the risks to our computer resources. The program provides FDA overseas travelers and investigators with temporary laptops and/or BlackBerrys to eliminate exposure of sensitive information. Additionally, FDA provides Foreign Travel Security Awareness Training to overseas travelers.

FDA is not aware of any corporate intelligence monitoring of FDA inspections, such as electronic surveillance of Internet transmissions from hotels where FDA investigators reside during inspections.

**2. How does FDA identify and classify trade secret and confidential information? Does the FDA consult with the company to determine whether certain information is a trade secret or whether certain information would be damaging to the company if disclosed? If not, why not? How would the FDA handle Freedom of Information Act (FOIA) requests that involve food industry trade secrets or confidential information? Would the FDA consult with the company who is the subject of the FOIA request to determine whether certain information potentially covered by the request was a trade secret or was otherwise highly confidential? If not, why not?**

FDA uses the definitions of trade secret and commercial or financial information that is privileged or confidential (referred to here and throughout this letter as CCI) in 21 CFR 20.61.

21 CFR 20.61 defines CCI as “valuable data or information which is used in one’s business and is of a type customarily held in strict confidence or regarded as privileged and not disclosed to any member of the public by the person to whom it belongs.” Examples of CCI include raw material supplier lists, finished product customer lists, and trace back information.

Trade secret information is also defined in 21 CFR 20.61. A trade secret is defined as a “commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort.” In order for information to be considered a trade secret, there must be a direct relationship between the trade secret and the manufacturing methods and processes. An example of a trade secret would be the formula for the natural flavorings in a carbonated soft drink.

The classification placed on a product, ingredient, or process by the company does not determine how it will be classified. Classifications are made based on the criteria outlined in 21 CFR 20.61.

During FDA inspections, FDA investigators may consult with the firm to determine what information they consider to be trade secret or proprietary. Many companies stamp records given to FDA investigators during inspections as “Trade Secret,” which FDA may use as a guide in any final determinations of its classification.

FDA processes FOIA requests, including those involving food industry trade secrets and CCI, pursuant to FOIA (5 USC 552) and FDA’s regulations in Title 21 of the CFR. FOIA Exemption 4 (5 USC 552(b)(4)) and 21 CFR 20.61 prohibit the release of trade secrets and CCI, and FDA’s FOIA staff review all records prior to release to redact any such non-public information from responsive records.

When processing FOIA requests that include trade secrets and CCI designated by the submitter, FDA follows Executive Order 12600 and its regulations at 21 CFR 20.61(d) and (e). As appropriate, the Agency consults with the submitter of the information; when the Agency receives a request for such records and determines that disclosure may be required, FDA will make reasonable efforts to notify the submitter about these facts. The notice will include a copy of the request, and it will inform the submitter about the procedures and time limits for submission and consideration of objections to disclosure. The submitter has five working days from receipt of the notice to object to disclosure of any part of the records and to state all bases for its objections. FDA will give consideration to all bases that have been stated in a timely manner by the submitter. Should FDA determine to release information that the submitter designates as non-public, the Agency would follow the procedure set forth in the executive order.

**3. How does FDA determine which personnel may access trade secret and confidential information? How does FDA ensure that unauthorized FDA personnel do not have access to trade secret and confidential information? Does the FDA conduct any “need to know” assessments? If yes, please describe. If not, why not?**

FDA Operating Divisions and senior officials that have responsibility and authority to handle trade secret and CCI make determinations about which FDA personnel are provided access and visibility. Regarding electronic access to information, two primary information security principles are observed in determining accessibility to an information system.

- Need to Know – A user should have access only to the information and resources necessary to complete the tasks that fulfill his or her role within an organization.
- Least Privilege – A user should be granted the most restrictive set of privileges needed for the performance of these authorized tasks.

Strict application of these two principles limits the possibility of unauthorized use of an information system or its data.

**4. Do FDA personnel undergo specific training on FDA procedures to protect trade secret and confidential information? If so, does this include FDA personnel in district offices and/or at CFSAN? If so, please explain the nature of that training.**

As mentioned in the response to Question 1, yes, all FDA personnel are required to complete annual Computer Security Awareness Training that outlines individual responsibilities for handling trade secret, company confidential, and other related information. Additionally, new employees receive generalized awareness briefings related to handling sensitive and confidential information.

FDA also provides substantive FOIA training to its employees. Full-time FOIA professionals are required to undergo training in FOIA. Program staff are offered training opportunities in FOIA, with Advanced FOIA and Introductory FOIA classes offered throughout the year, as well as upon request by specific Agency components. All FOIA training programs focus on the FOIA exemptions, including the exemption for trade secrets and CCI (i.e., FOIA Exemption 4). FOIA training is provided in person for staff in the Washington, D.C. area, and via webinar for staff located elsewhere. Training materials are maintained on the Agency's intranet for future reference and use.

**5. How are documents with trade secret and/or confidential information maintained (electronically or paper format)? What systems are in place to prevent unauthorized reproduction of a document with trade secret and/or confidential information? Does FDA have any tracking system that would enable the agency to know if a document was copied and distributed to an unauthorized person?**

All systems in use by CFSAN and ORA have received an Authorization To Operate, resulting from FDA's security authorization process performed by FDA's Chief Information Officer/Authorizing Official. The Authorization To Operate states that the security controls in place at the time of evaluation are in compliance with Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," and will remain in compliance throughout the system's development life cycle. In addition, information travelling from the FDA Field Offices to Headquarters is encrypted.

CFSAN maintains physical documentation through the DCC as well as throughout internal Program office file systems. Respective offices are responsible for managing any on-premise office physical records in accordance with FDA records management policy. When no longer required to support programmatic activities, documentation is released to the DCC for secure storage, preservation, and alignment with the appropriate federal records retention schedules. Physical records stored within the DCC are under lock and key and only accessible to authorized personnel.

CFSAN and ORA are in the process of reducing and eventually eliminating physical records retention in accordance with the eRecords Presidential memorandum, which is an Executive Branch-wide effort to update records management policies and practices. CFSAN has awarded a Fiscal Year 2015 contract to initiate the transfer of retained physical records to electronic format via the FDA records management system, Documentum. When requests for access to records are received by the DCC, any physical records requested are scanned and issued via email directly to only designated and approved personnel. The robust security tracking capabilities of the systems and applications FDA uses to access information will ensure that visibility to any confidential or trade secret information is granted to authorized individuals through secure HHS Personal Identity Verification (PIV) authentication and authorization protocols.

In 2015, ORA implemented a new system that electronically manages inspection reporting. Final inspection reports are transferred to Documentum. Information gathered and maintained in the system is protected through role-based user access. User accessibility and roles are reviewed on a semi-annual basis in order to make sure that approvals for information visibility are still valid and required.

As mentioned previously, inspection reports or other records still in paper format, which may or may not contain trade secret or CCI, are stored at FDA Field Offices in a document file room or in file cabinets kept under lock and key and are only accessible by FDA personnel with proper identification or access codes.

For any non-public information shared, including trade secret and/or CCI, FDA may be able to trace the origin of the request, as well as the initial receiver of the information provided, via email or postal tracking.

**6. How does FDA monitor the security of trade secret and confidential information in FDA's possession? For example, does FDA conduct security checks or audits? Have these been conducted at FDA district offices and/or CFSAN?**

As part of the FDA Security Authorization process, OIMT conducts periodic security assessments of FDA's network. In addition, OIMT monitors networks, systems, and applications for anomalies. In the event of an unauthorized disclosure of trade secret and/or CCI, OIMT provides analysis and support to FDA's Office of Criminal Investigations (OCI).

The Agency conducts bi-monthly security scans to detect and remediate vulnerabilities associated with computers, systems, networks, and applications.

Information security awareness training is required for all employees annually to maintain access to FDA networks and systems. Contract employees must be recertified on an annual basis to maintain access to FDA networks. These security checks and audits apply for both the FDA headquarters as well as the CFSAN and ORA field and satellite offices.

With regard to the security and monitoring of trade secrets stored in paper format, FDA personnel need an identification card/badge to gain entry into the offices where files are stored. File rooms or file cabinets that contain any records which may contain trade secret or CCI are under lock and key. Employees who are authorized to access this information have undergone security background checks conducted as part of their condition for employment.

**7. If a document with trade secret and/or confidential information is made public through unauthorized means, will FDA be able to determine which FDA personnel had custody of the document and was responsible for its disclosure?**

The Office of Internal Affairs (OIA) within OCI was established to conduct investigations of employee internal misconduct (60 FR 4417, January 23, 1995), and to provide a centralized liaison between FDA and the HHS Office of the Inspector General.

If an OIA investigation determines that a disclosure was intentional or done with reckless disregard by an FDA employee, it becomes a criminal matter. OCI/OIA would initiate a criminal investigation to determine the source of the unauthorized disclosure and the impact of the unauthorized disclosure. A number of factors would determine the ability to trace the source of the information, most importantly the number of FDA employees with access to the information. OCI/OIA would conduct interviews of FDA personnel who had access to the information. For any non-public information shared, including trade secret and/or CCI, FDA may be able to trace the origin of the request, as well as the initial receiver of the information provided, via email or postal tracking.

**8. How does the FDA monitor the electronic transmission of trade secret and confidential information?**

The FDA Systems Management Center is the central command and control center for the monitoring, triaging, and escalation of all detected, reported, or potential security incidents. The Systems Management Center monitors all networks, systems, and applications on an around-the-clock basis. In the event of an unauthorized disclosure of trade secret and/or CCI, OIMT's Information Security Staff conducts incident response and forensic analysis. In addition, they work closely with OCI and/or the HHS Office of the Inspector General on matters related to unauthorized disclosures.

**9. Has FDA performed a risk assessment for the security of trade secret and confidential information within the last 10 years? If so, please explain the nature of all assessments conducted and the results.**

To identify any weaknesses and security deficiencies, OIMT assesses security controls when they are initiated and on an annual basis thereafter to ensure information security principles are

built into CFSAN and Center-owned systems in accordance with the National Institute of Standards and Technology’s Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.”

**10. Are there ever any circumstances in which FDA could make an authorized disclosure of a company’s trade secret or commercial confidential information? If so, please describe those circumstances and the legal basis authorizing such disclosure.**

The circumstances in which FDA can make authorized disclosures of a company’s trade secret or CCI are limited. Many of these circumstances are contained in 21 CFR part 20, subpart E. These circumstances include, but are not limited to, disclosures: to Congress upon an authorized Congressional request (21 CFR 20.87); to the public to the extent necessary to effectuate a recall (21 CFR 20.91); to State and local government officials as part of cooperative law enforcement or regulatory efforts (21 CFR 20.88); and in response to a court order (21 CFR 20.83). In addition, FDA can disclose such information with the written permission of the owner of the information as well as to State officials who are part of the FDA Commissioning program and to other federal agencies that are part of HHS.

There are other circumstances, such as disclosures to the Government Accountability Office as consistent with 31 USC 716 and disclosures to foreign governments pursuant to memoranda of understanding executed in accordance with 21 USC 379(c), where such information is authorized to be shared.

Thank you, again, for contacting us concerning this matter. If you have further questions or concerns, please let us know. The same letter has been sent to your cosigner.

Sincerely,



Dayle Cristinzio  
Acting Associate Commissioner  
for Legislation

Enclosures

# Enclosure 1

## FDA Annual Security Awareness Training Section 2 of 10

### PROTECTING INFORMATION

It is estimated that more than 25% of the nation's gross domestic product is regulated by the FDA. To protect and promote the public health, the FDA is entrusted with valuable information that legally requires protection. Some of this critical and sensitive data includes:

- Intellectual property
- Trade secrets
- Proprietary information
- Company confidential information
- Personally Identifiable Information (PII)
- Protected Healthcare Information (HIPAA)
- Classified and acquisition information

Federal law and regulations require the FDA to protect sensitive information. All FDA system users are responsible for protecting information.

#### Protect Your Devices

One of the easiest ways to protect FDA information is not to let your FDA laptop or other system be lost or stolen. Treat your FDA laptop the way you would treat \$1,000 in cash. You probably wouldn't leave a pile of your money on the seat of your car, check it in your luggage at the airport, or walk away from it in a coffee shop would you? Lost, stolen, or unaccounted for devices may contain sensitive information worth far more than the replacement cost of the equipment.

#### Consequences of the OPM Breaches

In 2015, the Office of Personnel Management (OPM) revealed security breaches affecting millions of federal workers.

- Compromised personally identifiable information (PII) could be used for identity theft
- Security clearance applications contain data that could be used to blackmail or exploit federal employees such as:
  - Personal, family, business, and foreign national associates
  - Criminal history or past drug use
  - Financial, psychological and health information

**Source:** "Why The OPM Breach Is Such a Security and Privacy Debacle," Kim Zetter and Andy Greenberg, Wired, June 11, 2015

Some incidents of information loss, like the OPM breaches, are the result of hackers, but others are caused by avoidable human error. Careless mistakes like leaving a laptop unattended or clicking on a link

in a suspicious e-mail could result in the loss of sensitive information. As the saying goes: stop, think, then click.

### **Public versus Non-Public Information**

All FDA information, and information entrusted to FDA by third parties, is either public or non-public.

**Public information** has been explicitly approved as suitable for public dissemination. Examples of public information:

- Information brochures
- Press releases

**Non-public information** must be protected. Access to non-public information is restricted. Disclosure requires the approval of the information owner and, in the case of third parties, also a signed confidentiality agreement. Examples of non-public information:

- Employee performance reviews
- Commercial trade secrets
- Classified information

Click to see what Non-public Information includes.

- Information about FDA investigations and enforcement actions
- Time-critical information
  - Pre-award grant and contract data
  - Acquisition (pre-award)
  - Budget (pre-appropriation)
  - Pre-trip law enforcement travel and travel authorization data
- Proprietary information, such as research/scientific data
- Financial and personnel records
- Personally Identifiable Information
  - Records about individuals that require protection under the Privacy Act
  - Patient records protected by the Health Insurance Portability and Accountability Act (HIPAA)
  - Once referred to as Information in Identifiable Form (IIF)

### **Personally Identifiable Information (PII)**

PII can be public. For example:

- Names and other information about individual defendants in court cases
- Names and contact information for FDA staff

Most PII at FDA is non-public. To prevent security breaches of Personally Identifiable Information (PII), FDA uses controls including full-disk encryption for laptops and e-mail encryption. Everyone processing PII must know and follow the policies and procedures for storing, handling, and sharing PII. Specifically:

- Encrypt all electronic transfer of PII outside of the FDA network. Encrypt all electronic transfer of PII sent outside of the FDA firewall.
    - It is a best practice to encrypt ALL transfer of PII within or outside of the FDA network.
  - Shred physical PII when it is no longer needed.
  - Share PII only with authorized users that have a clear need to know the PII to perform their official duties.
  - Don't record or communicate PII unless there is a mission need to do so. Legacy forms and reports may call for or contain PII that is no longer needed for the action at hand--when this happens, either don't collect the PII or redact the PII before sending the information forward.
  - To report a Personally Identifiable Information (PII) incident, immediately contact the FDA Systems Management Center at:
    - E-mail: [FDA Systems Management Center@fda.hhs.gov](mailto:FDA_Systems_Management_Center@fda.hhs.gov)
    - Toll Free Number: 855-5FDA-SOC ( 855-533-2762 )
- For more information, see [Reporting a PII Breach](#)  (FDA Intranet Site).

### **Protected Health Information (PHI)**

The United States Health Insurance Portability and Accountability Act (HIPAA) defines Protected Health Information (PHI) as any information about health status, provision of health care, or payment for health care that can be linked to an individual. Protected Health Information is always non-public.

The FDA is not a HIPAA-covered entity. However, FDA personnel interact with HIPAA-covered entities (such as research hospitals) who may request that FDA apply HIPAA protection to information they provide.

HIPAA specifies eighteen identifiers associated with Protected Health Information, all of which are considered PII, such as medical record numbers, health plan beneficiary numbers, and medical device serial numbers and similar identifiers.

## ***FAST* FACTS**

Javelin's 2015 Data Breach Fraud Impact Report predicts that "between now and the end of 2018, data breaches involving healthcare, government and education will skyrocket. And the information compromised during these breaches will be much more devastating, long-term, than the card data we've seen compromised in the last 24 to 36 months via retail breaches such as Target and Home Depot. That's because in healthcare breaches, such as Anthem, or government breaches, such as the Internal Revenue Service and Office of Personnel Management hacks, personally identifiable information is the target, and it's selling in the underground for a much higher dollar amount than any of the cards compromised in retail attacks."

Source: "Breached PII: Growing Fraud Worry, New Account Fraud, Account Takeover Expected to Grow," Tracy Kitten, BankInfoSecurity, June 11, 2015

### **Context is Important**

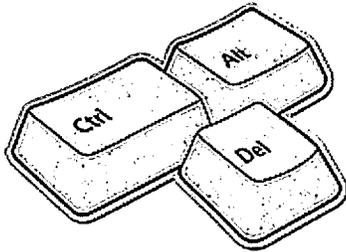
Sometimes bits of information put together can identify someone. For example, there may be only one thirty-six year old named Clementine in Glenelg, Maryland. None of this information is protected, but together it forms someone's identity. While this identity is based on information that is not protected, in some circumstances the information may merit protection as non-public. For example, if it is part of a list of individuals charged with a criminal offense.

## Protecting Information

Even with layers of technical controls, the FDA relies on you to protect sensitive information. A single careless action can compromise the best technical controls.

Click to learn how to reduce risk.

- Delete restricted data that you no longer need, including: drafts, old versions, extra copies of files, old e-mails, and attachments.
- Never share or discuss confidential or sensitive data with unauthorized individuals.
- Know who has access to network folders before you put confidential data there.
- Set up your workstation so that unauthorized people and passers-by cannot see the information on your monitor.



- Lock your computer (Press Control, Alt, and Delete at the same time, then select Lock Computer) when you walk away from it. This will prevent an unauthorized user from performing tasks or accessing information using your account.
- If you print FDA sensitive information, make sure you take it from the printer right away and keep it stored in a secure place.
- Protect all sensitive information and access only information that you need to do your job.

See threats to non-public information.

- Accidental disclosure – Unintended release of information due to careless actions such as sending to the wrong e-mail recipient, or e-mailing sensitive information to a compromised personal computer
- Court-ordered disclosure – Court orders to release information could have operational consequences
- Authorized user abuse (leaking) - Employees who publish non-public information on the Internet or leak it to a third party
- Hackers – Hackers may sell or publicize stolen information
- Industrial espionage – Companies or foreign government agencies may attempt to steal valuable sensitive information

- Malware - Programs that steal or alter information
- Spyware - Software that covertly collects information from a compromised computer
- Ransomware - Software that extortionists use to encrypt information and charge victims a fee to have the information unscrambled
- Blended threats – Techniques that combine criminal tactics and modern technology

## **Confidentiality**

Confidentiality is essential to our work. The FDA mission requires access to sensitive non-public data from businesses and consumers. We must also be able to discuss our concerns with the targets of our investigations. Irreparable hardship may occur when non-public information appears online, in the news media, or in the hands of anyone not authorized to know it.

If you have any questions about the FDA's policies on disclosure, please talk with your manager or the General Counsel's Office.

## **What are the Consequences?**

Loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals. It may also lead to identity theft or other fraudulent use of the information.

Theft of your PII can result in:

- Depleted bank or investment accounts
- Fraudulent credit card charges
- Loans or mortgages opened in your name
- Credit score problems
- Denial of credit
- Damage to reputation
- Harassment by bill collectors
- Employment problems; including people using your SSN to gain employment
- Tax identity theft and other problems with the IRS
- Medical identity theft, including inaccurate medical records
- Potential civil and criminal problems, including false arrest warrants and criminal records

Possible consequences for violations of IT security policies and procedures:

- Disciplinary action (up to the termination of employment)
- Civil action against FDA and/or the employee
- Criminal prosecution of the employee based upon the severity of the incident.
- **Individuals who fail to follow specific requirements of the Privacy Act may be charged with a misdemeanor and fined up to \$5,000 per violation.**

**OMB Requires Agencies to:**

**Immediately report all incidents involving PII** after discovering the incident. FDA employees should report all suspected computer security and privacy incidents to the FDA Systems Management Center at:

E-mail: [FDA\\_Systems\\_Management\\_Center@fda.hhs.gov](mailto:FDA_Systems_Management_Center@fda.hhs.gov)

Toll Free Number: 855-5FDA-SOC (855-533-2762)

This applies to incidents involving PII in electronic or physical form and does not distinguish between suspected and confirmed breaches.

**Encrypt sensitive information** that is:

- Accessed remotely
- Transported and/or stored offsite

### What are the Requirements for Protecting Non-public Information?

FDA employees and contractors are responsible for:

1. Knowing what information is non-public
2. Correctly handling and protecting non-public information
3. Reporting unauthorized disclosure of this information

## OPTIONAL REFERENCE LINKS

- [Secure Actions Checklist: Protecting Information](#)
- [How to Encrypt an E-mail Containing PII](#)  (FDA Intranet Site)
- [How to Report a Personally Identifiable Information \(PII\) Breach](#)  (FDA Intranet Site)
- [HHS-OCIO Policy for Information Systems Security and Privacy Handbook](#)  
- For Privacy-Related Questions
  - [Privacy Act Contacts](#)  for all HHS Divisions
  - [FDA Privacy Act Contacts](#)  (FDA Intranet Site)
- [Key Laws, Guidance, and Policy](#)
- [Fair Information Practice Principles \(FIPPs\)](#)
- [PII in the Information Life Cycle](#)
- [Classified Information](#) (defined)
- [HHS Cybersecurity Privacy page](#)  information on protecting PII and incident response
- [HHS Cybersecurity Privacy Resource Center](#)  tips on how to protect PII at work and at home

More Information on Laws and Regulations

- [22 Code of federal Regulations Chapter I, Subchapter M, Parts 120-130](#) 

- [15 CFR Parts 730-774](#) 
- [OMB Memorandum M-06-15](#)  "Safeguarding Personally Identifiable Information," May 22, 2006
- [OMB Memorandum M-06-16](#)  "Protection of Sensitive Agency Information," June 23, 2006
- [OMB Memorandum M-06-19](#)  "Reporting Incidents Involving Personally Identifiable Information," July 12, 2006



## **Enclosure 2**

**Office of the Chief Information Officer  
Office of the Assistant Secretary for Administration  
Department of Health and Human Services**

### **Rules of Behavior for Use of HHS Information Resources**

**July 24, 2013**

**Project:** HHS Standard Rules of Behavior  
**Document Number:** HHS-OCIO-2013-0003S

## Rules of Behavior for Use of HHS Information Resources

This Department of Health and Human Services (HHS or Department) standard is effective immediately:

The *Rules of Behavior for Use of HHS Information Resources* (HHS RoB) provides the rules that govern the appropriate use of all HHS information resources for Department users, including federal employees, contractors, and other system users. The HHS RoB, in conjunction with the *HHS Policy for Personal Use of Information Technology Resources*<sup>1</sup> (as amended), are issued under the authority of the *Policy for Information Systems Security and Privacy (IS2P)*.<sup>2</sup> The prior HHS RoB (dated August 26, 2010) is made obsolete by the publication of this updated version.

All new users of HHS information resources must read the HHS RoB and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HHS RoB. The HHS RoB may be presented to the user in hardcopy or electronically. The user's acknowledgement may be obtained by written signature or, if allowed per Operating Division (OpDiv) or Staff Division (StaffDiv) policy and/or procedure, by electronic acknowledgement or signature.

The HHS RoB cannot account for every possible situation. Therefore, where the HHS RoB does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.<sup>3</sup>

Non-compliance with the HHS RoB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include one or more of the following actions:

- Suspension of access privileges;
- Revocation of access to federal information, information systems, and/or facilities;
- Reprimand;
- Termination of employment;
- Removal or disbarment from work on federal contracts or projects;
- Monetary fines; and/or
- Criminal charges that may result in imprisonment.

HHS OpDivs may require users to acknowledge and comply with OpDiv-level policies and requirements, which may be more restrictive than the rules prescribed herein. Supplemental rules of behavior may be created for specific systems<sup>4</sup> that require users to comply with rules beyond those contained in this document. In such cases users must also sign these supplemental rules of behavior prior to receiving access to these systems and must comply with ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners must document any additional system-specific rules of behavior and any recurring requirement to sign the respective acknowledgement in the security plan for their systems. Each OpDiv Chief Information Officer (CIO) must implement a process to obtain and retain the signed rules of behavior for such systems and

---

<sup>1</sup> Available at: <http://www.hhs.gov/ocio/policy/index.html>

<sup>2</sup> Available at: <http://www.hhs.gov/ocio/policy/index.html>

<sup>3</sup> Refer to the Employee Standards of Conduct published by the U.S. Office of Government Ethics, available at: <http://www.oge.gov/Laws-and-Regulations/Employee-Standards-of-Conduct/Employee-Standards-of-Conduct>

<sup>4</sup> National Institute of Standards and Technology (NIST) Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, defines an "information system" as: "A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

## Rules of Behavior for Use of HHS Information Resources

must ensure that user access to such system information is prohibited without a signed acknowledgement of system-specific rules and a signed acknowledgement of the HHS RoB.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively implement their own system-specific rules.

These HHS RoB apply to local, network, and remote use<sup>5</sup> of HHS information (in both electronic and physical forms) and information systems by any individual.

Users of HHS information and systems must acknowledge the following statements:

I assert my understanding that:

- Use of HHS information and systems must comply with Department and OpDiv policies, standards, and applicable laws;
- Use for other than official assigned duties is subject to the *HHS Policy for Personal Use of IT Resources*, (as amended);<sup>6</sup>
- Unauthorized access to information or information systems is prohibited; and
- Users must prevent unauthorized disclosure or modification of sensitive information.<sup>7</sup>

I must:

### **General Security Practices**

- Follow HHS security practices whether working at my primary workplace or remotely;
- Accept that I will be held accountable for my actions while accessing and using HHS information and information systems;
- Ensure that I have appropriate authorization to install and use software, including downloaded software on HHS systems and that before doing so I will ensure that all such software is properly licensed, approved, and free of malicious code;
- Wear an identification badge (or badges, if applicable) at all times, except when they are being used for system access in federal facilities;
- Lock workstations and remove Personal Identity Verification (PIV) cards from systems when leaving them unattended;
- Use assigned unique identification and authentication mechanisms, including PIV cards, to access HHS systems and facilities;
- Complete security awareness training (i.e., HHS Information Systems Security Awareness Training) before accessing any HHS system and on an annual basis thereafter and complete any specialized role-based security or privacy training, as required by HHS policies;<sup>8</sup>
- Permit only authorized HHS users to use HHS equipment and/or software;
- Take all necessary precautions to protect HHS information assets<sup>9</sup> (including but not limited to hardware, software, personally identifiable information (PII), protected health information (PHI),

<sup>5</sup> Refer to the glossary of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* for definitions of local, network, and remote access.

<sup>6</sup> Available at: <http://www.hhs.gov/ocio/policy/index.html>

<sup>7</sup> HHS Memorandum: *Updated Departmental Standard for the Definition of Sensitive Information* (as amended) is available at: <http://intranet.hhs.gov/it/cybersecurity/policies/index.html>.

<sup>8</sup> HHS Memorandum: *Role-Based Training (RBT) of Personnel with Significant Security Responsibilities* (available at: <http://intranet.hhs.gov/it/cybersecurity/policies/index.html>) defines the types of positions requiring specialized training.

<sup>9</sup> HHS IT assets are defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS. Definition is adapted from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, *Guide for Conducting Risk Assessments*.

## Rules of Behavior for Use of HHS Information Resources

and federal records [media neutral]) from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and treat such assets in accordance with any information handling policies;

- Immediately report to the appropriate incident response organization or help desk (pursuant to OpDiv policy and/or procedures) all lost or stolen HHS equipment; known or suspected security incidents;<sup>10</sup> known or suspected information security policy violations or compromises; or suspicious activity in accordance with OpDiv procedures;
- Notify my OpDiv/StaffDiv Personnel Security Representative (PSR) when I plan to bring government-owned equipment on foreign travel (per requirements defined by the Office of Security and Strategic Information (OSSI));<sup>11</sup>
- Maintain awareness of risks involved with clicking on e-mail or text message web links; and
- Only use approved methods for accessing HHS information and HHS information systems.

### Privacy

- Understand and consent to having no expectation of privacy while accessing HHS computers, networks, or e-mail;
- Collect information from members of the public only as required by my assigned duties and permitted by the Privacy Act of 1974, the Paperwork Reduction Act, and other relevant laws;
- Release information to members of the public including individuals or the media only as allowed by the scope of my duties and the law;
- Refrain from accessing information about individuals unless specifically authorized and required as part of my assigned duties;
- Use PII and PHI only for the purposes for which it was collected and consistent with conditions set forth by stated privacy notices such as those provided to individuals at the point of data collection and published System of Records Notices; and
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual.

### Sensitive Information

- Treat computer, network and web application account credentials as private sensitive information and refrain from sharing accounts;
- Secure sensitive information, regardless of media or format, when left unattended;
- Keep sensitive information out of sight when visitors are present;
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with the *HHS Policy for Records Management*<sup>12</sup> and sanitization policies, or as otherwise lawfully directed by management;
- Access sensitive information only when necessary to perform job functions; and
- Properly protect (e.g., encrypt) HHS sensitive information at all times while stored or in transmission, in accordance with the *HHS Standard for Encryption of Computing Devices*.<sup>13</sup>

### I must **not**:

- Violate, direct, or encourage others to violate HHS policies or procedures;
- Circumvent security safeguards, including violating security policies or procedures or reconfiguring systems, except as authorized;

<sup>10</sup> Known or suspected security incidents involve the actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information maintained by or in the possession of HHS or information processed by contractors and third-parties on behalf of HHS.

<sup>11</sup> OSSI policies for foreign travel can be found at: <http://intranet.hhs.gov/security/ossi/foreign/index.html>

<sup>12</sup> Available at: <http://www.hhs.gov/ocio/policy/index.html>

<sup>13</sup> Available at: <http://intranet.hhs.gov/it/cybersecurity/policies/index.html>

## Rules of Behavior for Use of HHS Information Resources

- Use another person's account, identity, password/passcode/PIN, or PIV card or share my password/passcode/PIN;
- Remove data or equipment from the agency premises without proper authorization;
- Use HHS information, systems, and hardware to send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums;
- Exceed authorized access to sensitive information;
- Share or disclose sensitive information except as authorized and with formal agreements that ensure third-parties will adequately protect it;
- Transport, transmit, e-mail, remotely access, or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information;
- Use sensitive information for anything other than the purpose for which it has been authorized;
- Access information for unauthorized purposes;
- Use sensitive HHS data for private gain or to misrepresent myself or HHS or for any other unauthorized purpose;
- Store sensitive information in public folders or other insecure physical or electronic storage locations;
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information;
- Copy or distribute intellectual property including music, software, documentation, and other copyrighted materials without written permission or license from the copyright owner;
- Modify or install software without prior proper approval per OpDiv procedures;
- Conduct official government business or transmit/store sensitive HHS information using non-authorized equipment or services; or
- Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS information:
  - Antivirus software with the latest updates;
  - Anti-spyware and personal firewalls;
  - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access; and
  - Approved encryption<sup>14</sup> to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

I must refrain from the following activities when using federal government systems, which are prohibited per the *HHS Policy for Personal Use of Information Technology Resources*,<sup>15</sup> (as amended):

- Unethical or illegal conduct;
- Sending or posting obscene or offensive material;
- Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages;
- Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act;<sup>16</sup>
- Conducting any commercial or for-profit activity;
- Using peer-to-peer (P2P) software except for secure tools approved in writing by the OpDiv CIO (or designee) to meet business or operational needs;

---

<sup>14</sup> Refer to the *HHS Standard for Encryption of Computing Devices*, available at: <http://intranet.hhs.gov/it/cybersecurity/policies/index.html>.

<sup>15</sup> Available at: <http://www.hhs.gov/ocio/policy/index.html>.

<sup>16</sup> For additional guidance refer to <http://www.osc.gov/hatchact.htm> and 5 C.F.R. Part 2635: Standards of ethical conduct for employees of the executive branch.

Rules of Behavior for Use of HHS Information Resources

- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material;
- Creating and/or operating unapproved Web sites or services;
- Allowing personal use of HHS resources to adversely affect HHS systems, services, and co-workers (such as using non-trivial amounts of storage space or bandwidth for personal digital photos, music, or video);
- Using the Internet or HHS workstation to play games or gamble; and
- Posting Department information to external newsgroups, social media and/other other types of third-party website applications,<sup>17</sup> or other public forums without authority, including information which is at odds with departmental missions or positions. This includes any use that could create the perception that the communication was made in my official capacity as a federal government employee, unless I have previously obtained appropriate Department approval.

**APPROVED BY AND EFFECTIVE ON:**

\_\_\_\_\_/s/\_\_\_\_\_  
Frank Baitman  
HHS Chief Information Officer

\_\_\_\_\_  
July 24, 2013  
DATE

<sup>17</sup> Refer to the *HHS Policy for Managing the Use of Third-Party Websites and Applications*, available at <http://www.hhs.gov/ocio/policy/index.html>.

**SIGNATURE PAGE**

I have read the *HHS Rules of Behavior for Use of Information Resources* (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013, and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the Operating Division (OpDiv) Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name: \_\_\_\_\_  
(Print)

User's Signature: \_\_\_\_\_

Date Signed: \_\_\_\_\_

Digital Signature (optional):

The record copy is maintained in accordance with the General Records Schedule (GRS) 1, 18.a.