

MOU 225-74-8001

Memorandum of Understanding
Between The Consumer Product Safety Commission
and The Food and Drug Administration

The Food and Drug Administration (hereinafter called FDA) and the Consumer Product Safety Commission (hereinafter called CPSC) agree to the following:

Purpose: To provide a means by which CPSC may obtain access and use of certain FDA document files that contain privileged information and establish minimum requirements for a system to control and protect these documents.

Background: CPSC was formally established on May 14, 1973. A major component of that organization was the Bureau of Product Safety (BPS), formerly a part of FDA. BPS, having responsibility for hazardous products, produced regulatory documents that are maintained in FDA's central record repository. CPSC now has need to refer to those documents in order to assist in the implementation of the Consumer Product Safety Act (Public Law 92-573). The records referred to are intermingled, with records produced by other Bureaus of FDA, in FDA's Administrative Files (EIR's) maintained by the Records Section, Administrative Services Branch, Division of General Services, and thus it is impracticable to transfer BPS records to the CPSC pursuant to the Act.

I. Services to be Performed

A. FDA agrees to:

1. Loan administrative files upon request from CPSC.
2. Maintain a file charge-out and control system meeting the requirements specified in FDA Staff Manual Guide FDA h. 2280.6.
3. Release files only to those CPSC personnel identified in Article IV below.

B. CPSC agrees to:

1. Comply with all control and protection requirements specified in FDA Staff Manual Guide FDA h. 2280.6 – Protection of Privileged Information at Headquarters (copy attached).

2. Return all borrowed files, in tact, to FDA's Record Section within three (3) working days from charge-out date.

3. Pick up and return all files by messenger (control personnel).

II. Name and Address of Participating Agency

Consumer Product Safety Commission
Westwood Towers
5401 Westbard Avenue
Washington, D.C. 20016

III. Liaison Officers

A. Mr. William E. Sheridan
Director, Division of Contracts and Services
Office of Resource Utilization
Consumer Product Safety Commission
Telephone: 496-7668

B. Mr. E. A. Sturgis Hiller, Jr. Chief, Administrative Services Branch
Division of General Services
Associate Commissioner for Administration
Food and Drug Administration
Telephone: 443-3110

IV. CPSC Control Personnel

Upon approval and acceptance of this agreement, CPSC will provide FDA, in writing, the names of those personnel who will be authorized to pick up and return files. The names of those personnel are to be updated as necessary.

V. Period of Agreement

This agreement will become effective when accepted by both parties and will carry on for an indefinite period. This agreement may be modified by mutual consent of both parties or may be terminated by either party upon a thirty (30) day advance written notice to the other.

**Approved and Accepted
for the Consumer Product Safety Commission**
Signed by: Albert S. Dimcoff

Acting Director, Office of Resource Utilization
Date: July 6, 1973

**Approved and Accepted
for the Food and Drug Administration**

Signed by: Edward Steffee for Gerald F. Meyer
Acting Associate Commissioner for Administration
Date: June 28, 1973

FDA-MOU 74-1
Amendment No. 1

Purpose: The purpose of this amendment is to (1) effect a change in the Liaison Officer designation and (2) add a requirement to the scope of the agreement.

1. Under Article I, "Services to be Performed," add to Item B.2. the following:

When CPSC has a need for the permanent possession of records material, it may do so by making photocopies for their retention.

2. Under Article III entitled "Liaison Officers" change Item A. to read as follows:

A. Mr. Landy F. Thompson
Records Management Officer
Office of Resource Utilization
Consumer Product Safety Commission
Telephone: (301) 496-7033

Except as heretofore amended, all terms and conditions of this agreement remain in full force and effect.

**Approved and Accepted
for the Consumer Product Safety Commission**

Signed by: Albert S. Dimcoff
Director, Office of Resource Utilization
Date: March 18, 1974

**Approved and Accepted
for the Food and Drug Administration**

Signed by: Gerald F. Meyer

Associate Commissioner for Administration
Date: March 11, 1974

**DHEW REGIONAL BOUNDARIES
AND HEADQUARTERS
(map)**

PROTECTION OF PRIVILEGED INFORMATION AT HEADQUARTERS

1. Purpose
2. Policy
3. References
4. Definitions
5. Objectives
6. Responsibilities
7. Document Accountability
8. Document Protection
9. Document Reproduction
10. Document Destruction
11. Violations
12. Effective Date

Attachment A – Basic List of File Series that Contain Privileged Information

1. **PURPOSE.** This Guide establishes minimum requirements for a system to control and protect those documents which contain privileged information.

2. **POLICY.** As a regulatory agency of the United States Government, FDA and its employees will provide the necessary safeguards for the protection of privileged information. Such information will be released only to employees of the Agency unless otherwise authorized by law or the source of the information.

3. **REFERENCES.** Statutory requirements for safeguarding privileged information entrusted to the Agency are contained in the following:

- a. Section 301(j) Federal Food, Drug, and Cosmetic Act 21 U.S.C. 331(j)
- b. Section 359(d) Public Health Service Act 42 U.S.C. 263g(d)
- c. Section 360A(e) Public Health Service Act 42 U.S.C. 263(i)

4. DEFINITIONS.

a. **Privileged Information.** As used in this Guide, it refers to all information of a trade secret or privileged nature (manufacturing processes, patients' names, formulas, etc.) which is entitled to protection as defined by the above cited statutes. A basic list of files that are known to contain privileged information is attached (Attachment A).

b. **Major Organizations.** Offices of Associate and Assistant Commissioners, Offices of Legislative Services and Equal Employment Opportunity, Bureaus, the National Center for Toxicological Research and the Executive Director of Regional Operations.

c. **Control Officer.** That individual who has been designated in writing as having the responsibility for the organization's document control program.

5. OBJECTIVES

a. **Responsibility.** To establish individual responsibility for the accountability and protection of privileged information.

b. **Accountability.** To establish standards for effective systems to record the receipt and location of privileged information in FDA headquarters.

c. **Protection.** To establish standards for containers or areas used to store privileged information.

6. RESPONSIBILITIES.

a. **Associate and Assistant Commissioners and Directors of Major Organizations.** Associate and Assistant Commissioners and Directors of each major organization may delegate authority to carry out the provisions of this Guide to an operating level consistent with normal operating procedures. However, they retain overall responsibility for the protection and accountability of privileged information contained in records borrowed, maintained, or created by the organization. Their responsibilities include:

(1) Enforcing adherence to the provisions of this Guide.

(2) Designating an overall Control Officer and such assistant control by the organization.

(3) Insuring that Attachment A is supplemented to include any additional files or items of privileged information created or maintained by the organization.

b. **Control Officers.** Designated Control Officers are responsible for designing or strengthening and maintaining a system of accountability for those controlled official files under their control and reporting all lost files to the Policy Management Staff, ACA (CA-20).

c. **File Users.** Users of official files containing privileged information are responsible for complying with established procedures of accountability as prescribed by Control Officers and protecting borrowed files as provided for in this Guide.

7. DOCUMENT ACCOUNTABILITY. Privileged information received by an organization shall be identified in such a way that accountability for an individual file (e.g., folder, jacket or printout) can be maintained. Receipt records must indicate the number of volumes and copies received, and the control number assigned. The Control Officer shall establish and maintain an effective accountability system for privileged information files charged to the repository, other FDA organizations, or organizations outside FDA. Only designated file personnel shall be permitted to enter the file areas and charge-out controlled privileged information or file returned or incoming privileged information. Charge-out procedures shall include:

a. Charge-Out Files. When privileged information files are charged out, the borrower's name and the file identification of the borrowed file shall be recorded by repository personnel and a signature shall be obtained. Responsibility for the file remains with the last person whose signature appears on the routing slip as the document moves from one borrower to another, and this should be indicated in the charge-out record. The charge-out record shall be maintained in such a way that complete identification of the last borrower is possible if the file is not returned within 30 days.

b. Files Loaned to Other Major Organizational Units. Control systems shall provide that when a file is charged to an individual assigned to another major organization, the Control Officer of the borrower's organization shall be notified in writing of:

(1) The borrower's name and organizational sub-unit.

(2) The date of expiration of the control follow-up period. Subsequent verification of the location of the file shall be made through the Control Officer of the borrower's major organization.

c. Transferred Files. When privileged information files are permanently transferred to other FDA activities, the following information shall be maintained:

(1) The identification of the file.

(2) A notation that the file has been transferred.

(3) The location of the gaining organization.

(4) The date sent to the gaining organization.

(5) Verification that the file was received.

d. Control Follow-Up Period and Verification of Location. It is expected that most privileged information files will be returned to file within 30 days. Unless a repository determines that a shorter control follow-up period is necessary, follow-up shall be made to verify the location of each file which has been charged out over 30 days. Additional follow-up shall be made each succeeding 30 days until the file is returned. If continued use is necessary after a period of 90 days, the employee must specify retention in writing.

e. Report of Lost Files. It is necessary that missing files be promptly reported so that:

(1) Timely action can be taken to locate them.

(2) Corrective action can be taken to eliminate reoccurrence. To accomplish this, Control Officers shall immediately verify the location of charged files at the end of the control follow-up period. When files cannot be located, a report of lost files shall be prepared and forwarded to the Policy Management Staff within 15 days. The report of lost files shall consist of a memorandum from the Control Officer through the head of the organization to the Policy Management Staff, and shall contain the following information:

- (a) The file's identification and description of each missing file.
- (b) The name and organizational location of the individual to whom the file was last charged.
- (c) A resume of the efforts that have been made to locate the missing file.

8. DOCUMENT PROTECTION. The Director of each major organization shall ensure that privileged information for which he is responsible is properly protected. The security measures described below shall be established:

a. During Working Hours. Special protective measures are not required when FDA employees are in attendance and access to privileged information can be limited by such employees. Privileged information shall not be left unattended during working hours. If FDA employees cannot be present during working hours, the protective measures required for non-duty hours shall be used.

b. During Non-duty Hours. All privileged information must be placed in an approved secure files area or in an approved secure files container during non-duty hours. In accordance with the minimum standards set below, the Associate or Assistant Commissioner or the Director of each major organization is responsible for approving areas or containers to be used for the storage of privileged information during non-duty hours.

(1) Secure Files Areas. A secure files area is a room or rooms that can be locked during non-duty hours. In addition, a secure files area must be cleaned during working hours or under supervision of a guard if cleaned during non-duty hours. The Policy Management Staff will be kept advised of all such areas.

(2) Secure Files Containers. A secure files container includes any filing equipment that can be locked during non-duty hours (e.g., Power Files and Lektrievers, filing cabinets and shelf units).

c. Transmission of Privileged Information. It is necessary to maintain adequate protection of privileged information when in transit. Mail processing units shall use locked carts or mail bags for deliveries of privileged information. Privileged information which is to be transmitted via the U.S. Postal Service shall be sent by Registered Mail.

9. DOCUMENT REPRODUCTION. Privileged information may not be reproduced in whole or in part without the written approval of the Associate or Assistant Commissioner or the Director of the major organization. This authority may be delegated in writing to the unit's Document Control Officer. A record of the approval shall be maintained with the reproduced document. The protection and accountability of reproduced copies retained in an organization will be the same as that given the document from which they are reproduced. Accountability and charge-out records will be prepared

in accordance with paragraph 7 above. Procedures for destroying such documents shall be the same as for any other privileged information file or document.

10. DOCUMENT DESTRUCTION. Control Officers shall be responsible for establishing systems and procedures used in the destruction of privileged information within their jurisdiction. The physical destruction of privileged information shall be such that the contents are destroyed beyond recognition. The date of destruction and the name of the person responsible for it will be indicated in the document accountability record.

11. VIOLATIONS. The loss of privileged information may seriously hamper FDA in the conduct of its mission. Employees failing to comply with the provisions of this Guide and established control systems may be subject to personnel action commensurate with the seriousness of the violation. Supervisors shall report failure to comply with the provisions of this Guide to: (a) their Associate or Assistant Commissioner or the Director of their major organization for appropriate action, and (b) Director, Policy Management Staff.

12. EFFECTIVE DATE.

a. The name, location, and telephone numbers of the designated Control Officers will be provided to the Policy Management Staff (CA-20) by Associate and Assistant Commissioners and Directors of major organizations within thirty days after receipt of this Guide. Subsequent changes in such designations shall be submitted in writing to the Policy Management Staff within fifteen days after they occur.

b. Implementation of the provisions of this Guide shall begin upon receipt of this Guide and shall be completed within 60 days thereof.