Patulin''. This document is intended to make FDA offices and industry aware of FDA's guidance for enforcement concerning apple juice, apple juice concentrates, and apple juice products that contain patulin, a toxic substance produced by molds that may grow on apples, and that has been found to occur at high levels in some apple juice products offered for sale or import in the United States. The agency is also announcing the availability of a document entitled ''Patulin in Apple Juice, Apple Juice Concentrates, and Apple Juice Products'' (the draft supporting document).

DATES: Submit written comments by August 15, 2000.

ADDRESSES: Submit written requests for single copies of the draft CPG entitled ''Apple Juice, Apple Juice Concentrates, and Apple Juice Containing Products—Adulteration with Patulin'' and/or the draft supporting document entitled ''Patulin in Apple Juice, Apple Juice Concentrates, and Apple Juice Products'' to Michael E. Kashtock (address below). Send one self-addressed adhesive label to assist that office in processing your request. See the **SUPPLEMENTARY INFORMATION** section for electronic access to this document.

Submit written comments on the draft CPG and the draft supporting document to the Dockets Management Branch (HFA–305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Comments and requests for copies should be identified with the docket number found in brackets in the heading of this document.

FOR FURTHER INFORMATION CONTACT: Michael E. Kashtock, Center for Food Safety and Applied Nutrition (CFSAN) (HFS–305), Food and Drug Administration, 200 C St. SW., Washington, DC 20204, 202–205–5321, FAX 202–205–4422, e-mail: mkashtoc@cfsan.fda.gov.

SUPPLEMENTARY INFORMATION: FDA has developed a draft CPG on FDA's guidance for enforcement concerning apple juice, apple juice concentrates, and apple juice products that contain patulin. This document is intended to provide clear policy and regulatory guidance to FDA's field and headquarters staff with regard to such foods. In particular, if these products: (1) Contain patulin at or above 50 parts per billion (ppb) (the action level) based on the level found or calculated to be found in single strength apple juice, reconstituted single strength apple juice (if the food is an apple juice concentrate), or the single strength apple juice component of the product (if the food contains apple juice as an ingredient); and (2) the identity of patulin is confirmed by gas chromatography/mass spectrometry, then the FDA field enforcement office may consider whether to recommend legal action against such apple juice, apple juice concentrates, and apple juice products in interstate commerce, and it may consider whether to recommend detention of the same products when offered for import into the United States. For the purposes of this guidance, single strength juice is 100 percent juice that is unconcentrated (see 21 CFR 101.30(h)). The scientific basis for the 50 ppb action level is presented in the draft supporting document. The draft CPG also contains information that may be useful to the regulated industry and to the public.

FDA has included an import specimen charge in this draft CPG to assist its field personnel in recommending refusal of admission for imported goods when warranted. The fact that this draft CPG contains an import specimen charge (in addition to the customary specimen charge addressing regulatory action against food in domestic commerce) does not restrict any action FDA may take under circumstances addressed by other CPG's that do not have an import specimen charge, and it does not imply that FDA will not take action when warranted.

The agency has adopted good guidance practices (GGP's) that set forth the agency's policies and procedures for the development, issuance, and use of guidance documents (62 FR 8961, February 27, 1997). The draft CPG is being issued as a level 1 draft guidance consistent with GGP's. The draft CPG represents the agency's current thinking on its enforcement guidance concerning the adulteration of apple juice, apple juice concentrates, and apple juice products with patulin. It does not create or confer any rights for or on any person and does not operate to bind FDA, or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statute and regulations.

Interested persons may submit to the Dockets Management Branch (address above) written comments regarding the draft CPG and the draft supporting document by August 15, 2000. Two copies of any comments are to be submitted, except that individuals may submit one copy. Comments are to be identified with the docket number found in brackets in the heading of this document. Received comments, the draft CPG, and the draft supporting document may be seen in the Dockets Management Branch between 9 a.m. and 4 p.m., Monday through Friday. These two documents may also be accessed at the CFSAN home page on the Internet at http://www.fda.cfsan.gov.

Dated: June 8, 2000.

Margaret M. Dotzel,

Associate Commissioner for Policy.

[FR Doc. 00–15122 Filed 6–15–00; 8:45 am]

BILLING CODE 4160–01–F

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Health Care Financing Administration

Privacy Act of 1974; Report of Altered Systems

AGENCY: Department of Health and Human Services (HHS), Health Care Financing Administration (HCFA).

ACTION: Notice of the modification or alteration to 20 systems of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are correcting information provided in 20 HCFA systems of records specified in Appendix A. These systems are all related to research or demonstration projects under the control of the Office of Strategic Planning. We are deleting the published routine uses in the system of records listed in Appendix A and replacing them with four revised routine uses. The routine uses are being prioritized and renumbered accordingly. We are taking the opportunity to update those sections of the SORs that were affected by the recent reorganization. We are also updating the language in the administrative sections to correspond with language used in other HCFA system of records.

The primary purpose of the corrections to these systems is to shorten the language, make the routine uses easier to read, and provide clarity to HCFA's intention to disclose individual-specific information related to the purposes for which the information is being collected.

EFFECTIVE DATES: HCFA filed a correction to a system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on June 12, 2000. To ensure that all parties have adequate time in which to comment, the corrected systems of records, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is

later, unless HCFA receives comments that require alterations to this notice.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution (DDLD), HCFA, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 a.m.–3 p.m., eastern time zone.

FOR FURTHER INFORMATION CONTACT: Sydney P. Galloway, Privacy Act Coordinator, Systems, Technical, and Analytic Resources Group, Office of Strategic Planning (OSP), HCFA, Mailstop C3–24–07, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The telephone number is 410–786–6645.

SUPPLEMENTARY INFORMATION:

I. Collection and Maintenance of Data in the System

Agency Policies, Procedures, and Restrictions on the Routine Use

We are establishing the following policies, procedures and restrictions on routine use disclosures of information that will be maintained in these systems. In general, routine uses of these systems (or a subset thereof) will be approved for the minimum set of data elements in the record needed to accomplish the purpose of the disclosure after HCFA:

(a) Determines that the use or disclosure is consistent with the reason that the data is being collected, e.g., conducting research related to specific projects and demonstrations, and monitoring the quality of care provided to patients.

(b) Determines:

(1) That the purpose for which the disclosure is to be made can only be accomplished if the record is provided in individually identifiable form;

(2) That the purpose for which the disclosure is to be made is of sufficient importance to warrant the potential effect and/or risk on the privacy of the individual that additional exposure of the record might bring; and

(3) That there is a strong probability that the proposed use of the data would in fact accomplish the stated purpose(s).

(c) Requires the information recipient to:

(1) Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record; and

(2) Remove or destroy at the earliest time all patient-identifiable information.

(d) Determines that the data are valid and reliable.

II. Proposed Routine Use Disclosures of Data in the System

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a ''routine use.'' The proposed routine uses in this system meet the compatibility requirement of the Privacy Act. We are correcting the language in the following routine use disclosures of information maintained in these systems:

1. To an individual or organization for research, evaluation, or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects.

The collected data will provide the research, evaluation and epidemiological projects a broader, longitudinal, national perspective of the data. HCFA anticipates that many researchers will have legitimate requests to use these data in projects that could ultimately improve the care provided to Medicare patients and the policy that governs the care. HCFA understands the concerns about the privacy and confidentiality of the release of data for a research use. Disclosure of data for research and evaluation purposes may involve aggregate data rather than individual-specific data.

2. To agency contractors, or consultants who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity.

We contemplate disclosing information under this routine use only in situations in which HCFA may enter into a contractual or similar agreement with a third party to assist in accomplishing HCFA function relating to purposes for these systems of records.

HCFA occasionally contracts out certain of its functions when doing so would contribute to effective and efficient operations. HCFA must be able to give a contractor or consultant whatever information is necessary for the contractor or consultant to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or consultant from using or disclosing the information for any purpose other than that described in the contract and requires the contractor or consultant to return or destroy all information at the completion of the contract.

3. To a member of congress or to a congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

Beneficiaries sometimes request the help of a member of congress in resolving an issue relating to a matter before HCFA. The member of congress then writes HCFA, and HCFA must be able to give sufficient information to be responsive to the inquiry.

4. To the Department of Justice (DOJ), court or adjudicatory body when:

(a) The agency or any component thereof, or

(b) Any employee of the agency in his or her official capacity, or

(c) Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

(d) The United States Government is a party to litigation or has an interest in such litigation, and by careful review, HCFA determines that the records are both relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

Whenever HCFA is involved in litigation, or occasionally when another party is involved in litigation and HCFA's policies or operations could be affected by the outcome of the litigation, HCFA would be able to disclose information to the DOJ, court or adjudicatory body involved. A determination would be made in each instance that, under the circumstances involved, the purposes served by the use of the information in the particular litigation is compatible with a purpose for which HCFA collects the information.

III. Safeguards

The systems will conform with applicable law and policy governing the privacy and security of federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act (PRA) of 1995, the Clinger-Cohen Act of 1996, and OMB Circular A–130, Appendix III, ''Security of Federal Automated Information Resources.'' HCFA has prepared a comprehensive system security plan as required by the Office of Management and Budget (OMB) Circular A–130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18,

''Guide for Developing Security Plans for Information Technology Systems.'' Paragraphs A–C of this section highlight some of the specific methods that HCFA is using to ensure the security of this system and the information within it.

A. Authorized users: Personnel having access to the system have been trained in Privacy Act and systems security requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. In addition, HCFA is monitoring the authorized users to ensure against excessive or unauthorized use. Records are used in a designated work area or work station and the system location is attended at all times during working hours.

To assure security of the data, the proper level of class user is assigned for each individual user as determined at the agency level. This prevents unauthorized users from accessing and modifying critical data. The system database configuration includes five classes of database users:

- Database Administrator class owns the database objects, e.g., tables, triggers, indexes, stored procedures, packages, and has database administration privileges to these objects;
- Quality Control Administrator class has read and write access to key fields in the database;
- Quality Indicator (QI) Report Generator class has read-only access to all fields and tables;
- Policy Research class has query access to tables, but are not allowed to access confidential patient identification information; and
- Submitter class has read and write access to database objects, but no database administration privileges.

B. Physical Safeguards: All server sites have implemented the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the each system:

Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination which grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information System (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log-ons—Authentication is performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.
- Workstation Names—Workstation naming conventions may be defined and implemented at the agency level.
- Hours of Operation—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the agency level.
- Inactivity Log-out—Access to the NT workstation is automatically logged out after a specified period of inactivity.
- Warnings—Legal notices and security warnings display on all servers and workstations.
- Remote Access Services (RAS)—Windows NT RAS security handles resource access control. Access to NT resources is controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

There are several levels of security found in each system. Windows NT provides much of the overall system security. The Windows NT security model is designed to meet the C2-level criteria as defined by the U.S. Department of Defense's Trusted Computer System Evaluation Criteria document (DoD 5200.28–STD, December 1985). Netscape Enterprise Server is the security mechanism for all transmission connections to the system. As a result, Netscape controls all information access requests. Anti-virus software is applied at both the workstation and NT server levels.

Access to different areas on the Windows NT server are maintained through the use of file, directory and share level permissions. These different levels of access control provide security that is managed at the user and group level within the NT domain. The file and directory level access controls rely on the presence of an NT File System (NTFS) hard drive partition. This provides the most robust security and is tied directly to the file system. Windows NT security is applied at both the workstation and NT server levels.

C. Procedural Safeguards: All automated systems must comply with federal laws, guidance, and policies for information systems security as stated previously in this section. Each automated information system should ensure a level of security commensurate with the level of sensitivity of the data, risk, and magnitude of the harm that may result from the loss, misuse, disclosure, or modification of the information contained in the system.

IV. Effect of the Modified System of Records on Individual Rights

HCFA proposes to establish each system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in each system will be subject to the authorized releases in accordance with the routine uses identified in each systems of records.

HCFA will monitor the collection and reporting of all data. All information on beneficiaries is completed by the contractor and submitted to HCFA through standard systems located at the contractor sites. HCFA will utilize a variety of onsite and offsite edits and audits to increase the accuracy of all data.

HCFA will take precautionary measures (see item III. above) to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights including not collecting patient identifiable data for non-Medicare and non-Medicaid patients. HCFA will collect only that information necessary to perform the system's functions. In addition, HCFA will make disclosure of identifiable data from the modified system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act.

HCFA, therefore, does not anticipate an unfavorable effect on individual privacy as a result of the disclosure of information relating to individuals.

Dated: June 12, 2000.

Nancy-Ann Min DeParle,

Administrator, Health Care Financing Administration.

The corrections to the systems of records listed in Appendix A are as follows:

* * * * *

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

HCFA Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850.

* * * * *

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a ''routine use.'' Disclosure may be made:

1. To an individual or organization for research, evaluation, or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects.

2. To agency contractors, or consultants who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity.

3. To a member of Congress or to a Congressional staff member in response to an inquiry of the Congressional Office made at the written request of the constituent about whom the record is maintained.

4. To the Department of Justice (DOJ), court or adjudicatory body when:

(a) The agency or any component thereof, or

(b) Any employee of the agency in his or her official capacity, or

(c) Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

(d) The United States Government is a party to litigation or has an interest in such litigation, and by careful review, HCFA determines that the records are both relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

* * * * *

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

* * * * *

SAFEGUARDS:

HCFA has safeguards for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and systems security requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data.

In addition, HCFA has physical safeguards in place to reduce the exposure of computer equipment and thus achieve an optimum level of protection and security for the HCFA system. For computerized records, safeguards have been established in accordance with Department of Health and Human Services (HHS) standards and National Institute of Standards and Technology guidelines, e.g., security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management (IRM) Circular #10, Automated Information Systems Security Program, HCFA Automated Information Systems (AIS) Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised), Appendix III.

* * * * *

SYSTEM MANAGER(S) AND ADDRESS:

Director, Office of Strategic Planning, HCFA, Room C3–20–11, 7500 Security Boulevard, Baltimore, Maryland, 21244–1850. The telephone number is 410–786–6501.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, health insurance claim number, address, age, and sex, and for verification purposes, the subject individual's name (woman's maiden name, if applicable) and social security number (SSN). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2)).

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7).

* * * * *

Appendix A

09–70–0022 Municipal Health Services Program, HHS/HCFA/OSP

09–70–0030 National Long-Term Care Study Follow up, HHS/HCFA/OSP

09–70–0033 Person-Level Medicaid Data System, HHS/HCFA/OSP

09–70–0036 Evaluation of Competitive Bidding for Durable Medical Equipment Demonstrations, HHS/HCFA/OSP

09–70–0039 Evaluation of the Medicare Alzheimer's Disease Demonstration, HHS/HCFA/OSP

09–70–0040 Health Care Financing Administration Medicare Heart Transplant Data File, HHS/HCFA/OSP

09–70–0042 Medicare Cancer Registry Record System, HHS/HCFA/OSP

09–70–0045 Evaluation of the Arizona Health Care Cost Containment and Long Term Care Systems Demonstration, HHS/HCFA/OSP

09–70–0046 Home Health Quality Indicator System (HHQUIS), HHS/HCFA/OSP

09–70–0048 Monitoring of the Home Health Agency Prospective Payment Demonstration, HHS/HCFA/OSP

09–70–0049 Evaluation of the Home Health Agency (HHA) Prospective Payment Demonstration, HHS/HCFA/OSP

09–70–0050 The Medicare/Medicaid Multi-State Case Mix and Quality Data Base for Nursing Home Residents, HHS/HCFA/OSP

09–70–0051 Quality Assurance for the Home Health Agency (HHA) Prospective Payment Demonstration, HHS/HCFA/OSP

09–70–0052 Post-Hospitalization Outcomes Studies, HHS/HCFA/OSP

09–70–0053 The Medicare Beneficiary Health Status Registry Pilot, HHS/HCFA/OSP

09–70–0057 Evaluation of the Medicaid Extension of Eligibility to Certain Low Income Families Not Otherwise qualified to receive Medicaid Benefits Demonstration, HHS/HCFA/OSP

09–70–0058 Evaluation of the Medicare SELECT Program, HHS/HCFA/OSP

09–70–0059 The Medicaid Necessity, Appropriateness, and Outcomes of Care Study, HHS/HCFA/OSP

09–70–0063 Evaluation of the Medicaid Demonstration for Improving Access to Care for Substance Abusing Pregnant Women, HHS/HCFA/OSP

09–70–0066 Evaluation of, and External Quality Assurance for, the Community Nursing Organization (CNO) Demonstration, HHS/HCFA/OSP

[FR Doc. 00–15231 Filed 6–15–00; 8:45 am]

BILLING CODE 4120–03–P