Sang Min, Chun, President (Qualifying Individual).
Safe Harbor Logistics, Inc. , 5506 Fountain Bridge Lane, Houston, TX 77069. Officers: Marc J. Lawrence, President (Qualifying Individual), Melinda S. Lawrence, Director.

**Non-Vessel-Operating Common Carrier and Ocean Freight Forwarder Transportation Intermediary Applicants**

MBM International Logistics, LLC, 650 Atlanta South Parkway, Atlanta, GA 30349. Officers: Harold Hagans, Vice President (Qualifying Individual), Xiao Yan Mers, President.
Globe Shipping, Inc., 820 S. Garfield Ave., #202, Alhambra, CA 91801. Officers: Eric Qian, CEO (Qualifying Individual), Meili Ho, Secretary.
Marserve Inc., 15421 Vantage Pkwy West, #116, Houston, TX 77032. Officers: Michael Henley, Vice President (Qualifying Individual, Einar Eikrem, President.

**Ocean Freight Forwarder—Ocean Transportation Intermediary Applicants**

Infinity Logistics LLC, 100 N, Charles St., Suite 1200, Baltimore, MD 21201. Officers: Marjorie Shapiro, President (Qualifying Individual), James Shapiro, Vice President.
T & T Shipping Services of New York Inc., 820 Glenmore Avenue, Brooklyn, NY 11208. Officers: Patricia Williams, Vice President (Qualifying Individual), Patrick Turner, President.

Dated: September 8, 2006.

**Karen V. Gregory,**

*Assistant Secretary.*

[FR Doc. E6–15217 Filed 9–13–06; 8:45 am]
**BILLING CODE 6730–01–P**

## FEDERAL RESERVE SYSTEM

### Change in Bank Control Notices; Acquisition of Shares of Bank or Bank Holding Companies

The notification listed below have applied under the Change in Bank Control Act (12 U.S.C. 1817(j)) and § 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire a bank or bank holding company. The factors that are considered in acting on the notices are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The notices are available for immediate inspection at the Federal Reserve Bank indicated. The notices also will be available for inspection at the office of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received not later than September 29, 2006.

**A. Federal Reserve Bank of Kansas City** (Donna J. Ward, Assistant Vice President) 925 Grand Avenue, Kansas City, Missouri 64198–0001:

*1. Steve Burrage,* Antlers, Oklahoma; as co–trustee of the John L. Massey 2003 Family Trusts, to acquire voting shares of Durant Bancorp, Inc., and thereby indirectly acquire voting shares of First United Bank & Trust Company, both in Durant, Oklahoma.

Board of Governors of the Federal Reserve System, September 11, 2006.

**Robert deV. Frierson,**

*Deputy Secretary of the Board.*

[FR Doc. E6–15243 Filed 9–13–06; 8:45 am]
**BILLING CODE 6210–01–S**

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Office of the National Coordinator for Health Information Technology; American Health Information Community Confidentiality, Privacy, and Security Workgroup Meeting

**ACTION:** Announcement of meeting.

**SUMMARY:** This notice announces the second meeting of the American Health Information Community (''the Community'') Confidentiality, Privacy, and Security Workgroup in accordance with the Federal Advisory Committee Act (Pub. L. No. 92–463, 5 U.S.C., App.)

**DATES:** September 29, 2006 from 10 a.m. to 4:30 p.m.

*Place:* Hubert H. Humphrey Building (200 Independence Avenue, SW., Washington, DC 20201), Conference room 800 (you will need a photo ID to enter a Federal building).

*Status:* Open.

*Purpose:* At this meeting, the Community Confidentiality, Privacy, and Security Workgroup will receive information on identity proofing and user authentication as it relates to the breakthroughs currently being discussed by the Community's Consumer Empowerment, Chronic Care, and Electronic Health Record Workgroups.

The meeting will be conducted in hearing format, and the Workgroup will invite representatives who can provide information relevant to identity proofing and user authentication as it relates to the breakthroughs currently being discussed by the Community's Consumer Empowerment, Chronic Care, and Electronic Health Record Workgroups. The format for the meeting will include multiple invited panels and time for questions and discussion. The meeting will include a time period during which members of the public may deliver brief (3 minutes or less) oral public comment. Slots for oral comments by the public will be filled on the day of the meeting as time permits. To submit comments via e-mail, please send them to *Michele.Rollins@hhs.gov* (to ensure that your e-mail is received and appropriately filed, we ask that your explicitly put *''CPS Public Comment''* in the subject line of your e-mail) or mail your comments to Michele Rollins, Office of the National Coordinator (ONC), 330 C Street, SW., Suite 4090, Washington, DC 20201.

**SUPPLEMENTARY INFORMATION:** The Community's Confidentiality, Privacy, and Security (CPS) Workgroup will undertake steps to evaluate instances where health information technology (health IT) has shifted the CPS paradigm, as well as where policy (due to evolving technology) have become unclear or allow for varied interpretation.

The first two issues before the CPS workgroup (identity proofing and user authentication) were chosen because of their foundational importance to any security initiative. Inextricably linked, both issues need discussion in order to determine how authorized entry is governed to a new technology product, service, or infrastructure. In typical workflows, identity proofing and user authentication are the first of many processes completed in health care environments, followed shortly thereafter by other more complex activities such as access control, data management, information matching and transmission, and information assurance (data integrity, business continuity, etc.).

There is no one solution for identity proofing and user authentication. As health IT evolves, we expect that methods for identity proofing and user authentication will evolve as well. Certain types of health IT products may require more stringent methods while others may not, and understanding these tradeoffs will be critical to determining CPS policies. Deciding how to prove (with some degree of confidence) that someone is who they claim to be, followed by a repeatable authentication process, are necessary steps to ensure that an authorized person or entity can access a health IT product or service in a private and secure manner.

In an effort to inform members of the public responding to the questions posed for testimony, we are defining

identity proofing and user authentication. For the purposes of the CPS hearing, identify proofing should be understood to mean *the process of providing sufficient information (e.g., identity history, credentials, and documents) to correctly and accurately verify and establish an identity to be used in an electronic environment (e.g., over the Internet).* For many everyday processes such as applying for a passport or driver's license, identity proofing takes place. To be granted the rights associated with a passport or driver's license, one first needs to provide documents to prove one's identity (*e.g.,* birth certificate). This same principal exists to control access to electronic systems, and it is the intent of this hearing to discuss the types of identity proofing used or recommended to gain access to certain health IT products or services.

For the purposes of the CPS hearing, user authentication should be understood to mean *the process of reliably verifying a claimed or presented identity, often used as way to grant authorized access to data, resources, and other network services.* User authentication takes place after an identity has been successfully proofed (verified by the appropriate authority) and a credential representing that proofed identity has been assigned to an individual. This does not mean the assignment of a unique identifier, but rather it refers to the method any system uses (in a unique way) to differentiate its users (*e.g.,* a separate username) and challenge the user's ability to prove that they are who they claim to be (*e.g.,* knowledge of a password associated with the username).

While responding to the questions below, it is recommended that each response identify (1) The risks and benefits associated with a particular identity proofing and/or user authentication method; (2) the potential costs and/or barriers associated with the method's implementation; and (3) if feasible, quantify the risks, benefits, costs, or barriers discussed in parts 1 and 2, with respect to a health care consumer, provider, other entity, or all. *Responses should be particularly focused on the Community's breakthroughs (pre-populated and consumer-directed medication history and registration summary as part of a personal health record (PHR), access to current and historical laboratory results and interpretations in an electronic health record (EHR), and secure messages between patients and their clinicians).* Where possible, please provide references to any peer reviewed literature that has informed your response.

1. Does an in-person identity proofing process provide greater benefit than automated, on-line processes, or vice-versa? Please explain.

2. Identify and particular concerns regarding the type of information collected for identity proofing or the storage of such information.

3. Should there be different identity proofing and user authentication processes for:

a. A patient versus a clinician. If yes, please explain and identify the scenario;

b. The primary user of a PHR versus a proxy for that user?

4. Are there other industry policies and practices related to identity proofing and user authentication and could be used successfully in any of the Community identified breakthroughs (see above)? If so, please described these policies and specify how these could be implemented in a way that would minimize the risks and maximize the benefits as well as how they would compare to alternative methods in terms of risks, benefits and feasibility of implementation.

5. What is the appropriate balance of access to medical information in electronic form (through the use of stronger identity proofing and user authentication) against the privacy concerns of the consumer/patient? If possible, please discuss comparable programs/efforts in the past that have been successful in doing this?

6. What/how do you see the HHS's role, if any, in establishing guidelines for the health care industry with respect to identity proofing and user authentication? Or should the industry self-police in this area?

7. If private industry EHR or PHR services were to import data from Federal agencies (who are required either by statute or policy to protect data in certain ways), would it be reasonable to expect that the EHR or PHR service provided would comply with Federal information security practices?

8. Should the health care industry adopt the concept of multiple assurance levels when performing identity proofing and user authentication functions, similar to what OMB has defined for the Federal Government in OMB Memorandum M–04–04? When responding to this question, please cite, if possible other models that may exist specifically for health care?

9. Based on your experience (personal/organizational) discuss how identity proofing and user authentication are currently addressed in the Personal Health Record (PHR) market from a technical, policy, and implementation perspective. Please ensure that your answers identify:

a. How the type of PHR (i.e., who provides/sponsors the PHR) could impact the identity proofing and user authentication method chosen;

b. Who is capable of providing data to the PHR;

c. The potential impact the type of data (which may vary in levels of perceived sensitivity, e.g., a medication history that lists a drug for an ear infection versus a drug for HIV) could have on the identity proofing and user authentication method chose; and

d. How data is entered into the PHR, for example, by a health care consumer, or from a provider through a ''push model'' where data is automatically sent to the PHR without a request by the consumer.

10. Based on your experience (personal/organizational) with EHR technology, that can at a minimum provide access to current and historical laboratory results and interpretations, should identify proofing and user authentication methodologies (technical, policy, and implementation) differentiate based upon:

a. The reception method of the data

i. For example: Accessing a laboratory's secure Web site for results and typing them into a patient's EHR vs. automatic population from the lab to the EHR; and

b. The interconnectivity of the EHR

i. For example: A doctor in a large health care system may be able to query another provider's EHR for data as opposed to querying the lab directly.

Written testimony submitted by the public is not required to address all of the questions listed above, and answers to any or all of the questions will be accepted so long as they comply with the following testimony guidelines. Persons wishing to submit written testimony (*which should not exceed eight double-spaced typewritten pages*) should endeavor to submit it by September 29, 2006.

If you have special needs for the meeting or require further assistance, please contact (202) 690–7151 and reference the CPS meeting.

The meeting will be available via Web cast at *www.eventcenterlive.com/cfmx/ec/login/login1.cfm?BID=67* [Room Number: 8285166].

**Judith Sparrow,**

*Director, American Health Information Community, Office of Programs and Coordination, Office of the National Coordinator for Health Information Technology.*

[FR Doc. 06–7657 Filed 9–13–06; 8:45 am]

**BILLING CODE 4150–24–M**

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Centers for Disease Control and Prevention

**[60Day-06–06BO]**

### Proposed Data Collections Submitted for Public Comment and Recommendations

In compliance with the requirement of Section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995 for opportunity for public comment on proposed data collection projects, the Centers for Disease Control and