DEPARTMENT OF HEALTH & HUMAN SERVICES
200 Independence Avenue, SW
Washington, DC 20201

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF THE ADMINISTRATOR

Date: July 23, 2013

To: Howard Shelanski
Administrator, OIRA

From: Marilyn Tavenner,
Administrator

Subject: Request for Emergency Clearance of the Paperwork Reduction Act Package for the State Health Insurance Exchange Security Incident Reporting

Emergency Justification

The Centers for Medicare & Medicaid Services (CMS) is requesting that an information collection request for *State Health Insurance Exchange Security Incident Reporting* to be processed under the emergency clearance process associated with Paperwork Reduction Act of 1995 (PRA), specifically 5 CFR 1320.13(a)(2)(i). Public harm is reasonably likely to occur if the normal, non-emergency -clearance procedures are followed. The approval of this data collection process is essential to ensuring that Information Security (IS) incidents, which also include Personally Identifiable Information (PII) and Protected Health Information (PHI), are captured within the specified timeframe. In absence of this change, a significant number of incidents will not be detected; therefore causing harm and potential risk to the public's identity with identity fraud. Additionally, in accordance with 5 CFR 1320 13 (a)(2)(iii), a statutory implementation date of the Affordable Care Act, which is October 1, 2013, will be missed, if the normal clearance procedures are followed. Incidents could potentially occur on this statutory date; therefore, the reporting capability must be in place for States to inform CMS should an incident occur during this time.

Background

Reporting Security Incidents

An IS incident is an observable occurrence in a network or system, e.g., detected probes, infections prevented, log reviews, etc. Examples of events include an unplanned system reboot, a

system crash, and packet flooding within a network. Events sometimes provide indication that an incident is occurring. An incident becomes a breach when there is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information or personal health information, whether physical or electronic.

A Security Incident is a reportable event that meets one or more of the following criteria:

- The successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system processing information on behalf of Centers for Medicare Medicaid. The information also reflects on behalf of the following agencies; Internal Revenue Service, Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management and Veterans Health Administration. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the public's data at risk of unauthorized access, use, disclosure, modification, or destruction.

- An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

A reportable event is anything that involves: (1) a matter that a reasonable person would consider a violation of criminal, civil or administrative laws applicable to any Federal Health Care Program; or (2) integrity violations, including any known probable or suspected violation of any contract term or provision. A reportable event may be the result of an isolated event or a series of occurrences. Reportable events that are subject to reporting under these procedures include events that occur at the States, contractor site/system or any of its subcontractors, consultants, vendors or agents.

State Responsibilities Regarding Incident Reporting

CMS has implemented a Computer Matching Agreement (CMA) with the State-Based Administering Entities (AEs). This agreement establishes the terms, conditions, safeguards, and procedures under which CMS will disclose certain information to the AEs in accordance with the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act (Public Law 111-152), which are referred to collectively as the Affordable Care Act (ACA), amendments to the Social Security Act made by the ACA, and the implementing regulations. The AEs, which are state entities administering

Insurance Affordability Programs, will use the data, accessed through the CMS Data Services Hub (Hub), to make Eligibility Determinations for Insurance Affordability Programs and certificates of exemption.

AEs shall report suspected or confirmed incidents affecting loss or suspected loss of PII within one hour of discovery to their designated CCIIO State Officer who will then notify the affected Federal agency data sources, i.e., Internal Revenue Service, Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management and Veterans Health Administration. Additionally, AEs shall contact the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards within 24 hours of discovery of any potential breach, loss, or misuse of Return Information.

Timeline

August 2, 2013

- Target publication date for emergency 30-day Federal Register (FR) notice.
- Draft PRA package posted to CMS PRA web site
- PRA package formally submitted to OMB

September 2, 2013

- End of 30-day public comment period (The 30-day comment period actually ends 9/1, but it must end on a business day.)

September 3, 2013

- Start of OMB review period

September 15, 2013

- Requested date of OMB approval