National Committee on Vital and Health Statistics
Subcommittee on Privacy, Confidentiality & Security

CMS WRITTEN TESTIMONY

JUNE 9, 2009

Members of the Sub-Committee, my name is Chris Gayhead. I am the CMS Project Officer for the MyPHRSC Personal Health Record pilot. It is my pleasure to testify before you today about the South Carolina pilot, and the privacy and security standards we implemented along the way. As you already know, the growth of the Internet, web technologies, and other electronic tools are allowing the public to become more informed and actively engaged in their health care than was possible in the past. The Medicare population and their families are beginning to use these new technologies to get information about conditions and track medication history. CMS is using PHR pilots to explore different ways of making Medicare claims data available to Medicare beneficiaries electronically.

A few years ago, on August 16, 2005, CMS published a Request for Information (RFI) to obtain public feedback on our role regarding PHRs. We asked for their thoughts as to what CMS's role should be with PHRs, Technology and Standards, PHR Data Content, Marketing and Training, and Privacy and Security of Information. Briefly, we were told that CMS's role should be limited to that of providing data to outside PHR vendors, that is CMS should not develop its own PHR tool. Survey respondents further told us that enabling beneficiaries to understand and manage their health care should lead to improved quality and efficiencies in their care. They also thought that it would be critical for beneficiaries (or other authorized parties) to control the input and output of their PHRs.

We designed a series of Pilot PHR projects that would allow CMS to understand the feasibility of transmitting data from our claims systems to the PHR, to educate beneficiaries about PHRs, and to determine which features and functions PHR users found most valuable over time. MyPHRSC is one of the pilots designed to respond to those issues. It was the first pilot to offer a PHR to Medicare fee-for-service beneficiaries and the first time we have conducted extensive outreach to encourage PHR uptake. The lessons learned from the pilot could help inform future communications about PHRs, and create marketing and training packages that encourage use of PHRs throughout the Medicare program. So, our primary goal for creating MyPHRSC was to understand how to reach out and communicate with beneficiaries that might use PHRs. In doing so, we tied the PHR by contract to CMS. That meant that we were required to make MyPHRSC conform to CMS standards for privacy and security. We recognize that the Federal standards set a high bar for privacy and security. Many PHR products are not required to meet this standard, and many do not. However, we think that there can be some value in talking about the security and privacy we did implement, as a measure of what standards PHRs might consider.

QSSI, a Maryland based software company won the bid to be the prime contractor for the MyPHRSC pilot. Together with its subcontractors, HealthTrio, Palmetto GBA, and IBM, the company has worked with us to create MYPHRSC as a pilot that provides an on-line PHR to Medicare beneficiaries using of a commercial electronic PHR. MyPHRSC is only available to FFS beneficiaries in South Carolina. The system populates the PHR with two years of Medicare claims data for beneficiaries who elect to participate in the Pilot. Updated daily, the health record provides the beneficiary with one place to track their medical history. Additional information can be added manually, and the PHR provides helpful resources to understand diagnoses, and conditions. MyPHRSC is different from Medicare PHR Choice in that

MyPHRSC is tethered to CMS and its computer systems and users must adhere to CMS Information Security Policies, Standards, and Procedures as well as the HIPAA and FISMA requirements. Beneficiaries that access MyPHRSC consent to monitoring, recording, and auditing activities that CMS performs as part of the pilot evaluation, but we do not access their personal data in a way that identifies a beneficiary and their medical information.

Through a partnership with the Department of Defense (DoD), TRICARE Management Activity (TMA), TRICARE for Life pharmacy data became available for registered users in January 2009. Registered users may elect to have TRICARE for Life pharmacy data populated into their Personal Health Record through a second authorization once they enter the tool. Both CMS and the TMA adhere to their respective agency's Privacy and Security Plans.

MyPHRSC PRIVACY

MyPHRSC fully complies with the requirements of the HIPAA privacy and security rules required by CMS. We required the following documents and evidence from the prime contractor, QSSI and its subcontractors HealthTrio, Palmetto, and IBM:

- A current Privacy Policy and Notice of Privacy Practices;
- A written policy for data destruction and disposal following a beneficiary's death or decision to discontinue use of the PHR;
- Written policies and procedures for securing an individual's authorization to create and populate a PHR.
- Written policies and procedures of the methods used to authenticate beneficiaries and authorized representatives;
- Proof of necessary data use agreements with CMS and other business partners.
- Signed statement from Privacy and/or Security officer, or other designated official affirming compliance with the HIPAA Privacy and Security rules;

Additionally, QSSI and its partners were required to meet the requirements of the CMS Information Security Program. The policies, standards, and procedures that govern the pilot were obligated to conform to the CMS Information Security Program (www.cms.hhs.gov/informationsecurity) in order to: (1) enable CMS' business processes to function in an environment with adequate security protections, and (2) meet the security requirements of federal laws, regulations, and directives, including the Privacy Act of 1974 (as amended), HIPAA, and FISMA, as well as various rules, regulations, policies, and guidance developed by DHHS, OMB, Homeland Security, and NIST. These policies include:

- **The CMS Policy for the Information Security Program.** This policy aims to reduce the risk, and minimize the effect of security incidents and establishes the ground rules under which the CMS shall operate its information systems. All CMS employees, contractor(s), sub-contractor(s), and their respective facilities supporting CMS business missions shall observe the individual policy statements. Some policies are explicitly for persons with a specific job function, e.g., the System Administrator;

otherwise, all personnel supporting CMS business functions shall comply with the policies. The CMS IS Program Policies address the reduction in risks to information resources through adoption of preventive measures and controls designed to detect any errors that occur.

- **The CMS Information Security Acceptable Risk Safeguards (ARS)**. The ARS reflects the minimum thresholds for information security controls based on the NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, and NISP SP 800-63, *Electronic Authentication Guidelines*. These controls must be implemented to ensure that all CMS systems meet a minimum level of information security.

- **The CMS Information Security (IS) Risk Assessment (RA) Methodology.** This methodology presents a systematic approach for the Risk Assessment (RA) process of information systems within the CMS environment. The IS RA provides an evaluation of current security controls to safeguard against the identified threat/vulnerability pairs and the resulting risk levels; and the recommended safeguards to reduce the system's risk exposure with a revised residual risk level once the recommended safeguards are implemented.

- **The CMS System Security Plan Methodology**. This methodology is intended to serve as a tool for System Owners/Managers and System Maintainer/Managers in determining the SSP requirements of General Support Systems (GSS), Major Application (MA) systems and applications. The SSP documents the current level of security within the system and is evaluated by the CMS Chief Information Officer (CIO). Based on those controls currently implemented and documented in its SSP, the CIO determines whether or not the system will be granted authorization to process, i.e., accreditation. Similarly, the SSP forms the primary reference documentation for testing and evaluation, whether by CMS, the Government Accountability Office, the Inspector General, or other oversight bodies.

- **CMS Information Security Contingency Planning**. IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted IT services: restoring IT operations at an alternate location, recovering IT operations using alternate equipment, or performing some or all of the affected business processes using non-IT (manual) means (typically acceptable for only short-term disruptions). Each system must be covered by a current contingency plan and the plan must be tested on an annual basis.

- **CMS Security Test & Evaluation Reporting Standard**: Must be used when documenting the results of Information Security testing. The Reporting Standard for

IS Testing is currently under revision due to recently issued directives from the OMB and NIST.

PUBLIC PERCEPTION OF PRIVACY

The public is very interested in the privacy of their data. Throughout the 119 events planned or attended by MyPHRSC staff, the public consistently asks about data security, data privacy, and whether or not "big brother" will watch them if they choose to participate in the project. Generally, the public is satisfied when we explain to them that strict Federal Requirements protect the project. In most cases, people are satisfied to know that the project meets the Federal Requirements for data Privacy and Security. There are cases, however, where individuals comment that they have a general distrust of the internet and using electronic means to communicate their information. These individuals are less concerned with the privacy and security elements of the PHR project and more concerned with a general distrust of the computer and the internet.

SNOMED/SENSITIVE INFORMATION

ICD9 codes are translated into SNOMED CT data so that beneficiaries have the ability to understand their claims data. The SNOMED standard mapping has been extended by HealthTrio's internal experts in order to ensure the mappings are relevant. SNOMED coding provides a mechanism to tie together data that is otherwise unrelated. For example, self-entered medication data is not tied to Illness condition data. Without creating a mechanism that provides a relationship to the data, it is difficult to know which medications are associated with which diseases. So SNOMED helps to maintain privacy even when a user may not recognize that a certain medication suggests a diagnosis.

Users can allow trusted members of their health care team, family or people they trust to have access to their MyPHRSC records (e.g., Authorized Representatives). By having SNOMED tie the unrelated data together , the PHR allows the creation of Sensitive Data Categories. The PHR default setting hides restricted data classes and restricted functional areas;

- **Data Class** - Sexually Transmitted Diseases, Mental Health, Contraceptive Issues, Alcohol Abuse, Sexual Assault, Drug Abuse, Abuse or Neglect, Aids, Reproductive Health, HIV, Genetic Testing

- **Functional Area** - Claims, Permissions, and Social History

SUMMARY

Although the CMS PHR Pilot project in South Carolina was not developed specifically to test which privacy and security methods and standards were most appropriate for protecting beneficiary information, the pilot may provide a blue print of useful information on the steps necessary for a PHR that wishes to apply Federal Privacy and Security standards. The pilot has taught us that Privacy and Security requirements are best thought about and planned into the project from the very beginning. If this happens, adequate security and privacy standards can be clearly defined and communicated in a way that can create confidence that the safe handling of private information that beneficiaries have come to expect from Medicare is preserved. Building trust in the community has proved important in uptake and utilization of the PHR. Registered users of MyPHRSC have told us repeatedly that they are very interested in their care and managing their health care on-line. They are pleased to have access to the information available to them in the PHR. However, they are not willing to sacrifice the privacy and security of their information for the convenience of having on line access. We think that MyPHRSC has implemented a Federal standard of privacy and security that organizations might look to in the future when planning to bring a PHR online and it sets an example of how to re-organize existing policies and procedures to conform to Federal standards.