

FORTNEY PETE STARK, CALIFORNIA, CHAIRMAN
SUBCOMMITTEE ON HEALTH

LLOYD DOGGETT, TEXAS
MIKE THOMPSON, CALIFORNIA
RAHM EMANUEL, ILLINOIS
XAVIER BECERRA, CALIFORNIA
EARL POMEROY, NORTH DAKOTA
STEPHANIE TUBBS JONES, OHIO
RON KIND, WISCONSIN

DAVE CAMP, MICHIGAN
SAM JOHNSON, TEXAS
JIM RAMSTAD, MINNESOTA
PHIL ENGLISH, PENNSYLVANIA
KENNY C. HULSHOF, MISSOURI

CHARLES B. RANGEL, NEW YORK, CHAIRMAN
COMMITTEE ON WAYS AND MEANS

JANICE MAVS, CHIEF COUNSEL AND STAFF DIRECTOR
CYBELE BJORKLUND, SUBCOMMITTEE STAFF DIRECTOR

BRETT LOPER, MINORITY STAFF DIRECTOR
CHARLES CLAPTON, SUBCOMMITTEE MINORITY

Congress of the United States
U.S. House of Representatives
COMMITTEE ON WAYS AND MEANS

WASHINGTON, DC 20515

SUBCOMMITTEE ON HEALTH

August 6, 2008

Douglas J. Reding, MD, MPH, FACP
Oncologist/Hematologist
Vice President, Marshfield Clinic
1000 North Oak Ave
Marshfield, WI 54449-5777

Dear Dr. Reding:

As a follow up to the Health Subcommittee hearing on promoting the adoption and use of health information technology on July, 24th 2008; please respond to the following questions for the record.

Questions from Ranking Member Camp:

1. I understand that you have had a chance to review the health IT bill I introduced last month.

Are there provisions in my bill that you believe should become law?

2. I understand that the Marshfield Clinic is just one of many hospital, clinic, and physician groups that have expressed their concerns about the privacy language in H.R. 6357.

What impact do you feel this language would have on your clinic's ability to implement care and quality improvement programs as well as to monitor and prevent fraud?

3. Do you feel the current HIPAA protections sufficiently guard patient privacy as it relates to electronic records?

What steps does the Marshfield Clinic take to ensure that information found patient's electronic records are kept private and used appropriately?

How does the Marshfield Clinic deal with employees who improperly access medical records?



MARSHFIELD CLINIC

August 19, 2008

Carrie Breidenbach
Hearing Clerk
Committee on Ways and Means
United States House of Representatives
Washington, DC 20515

Dear Ms. Breidenbach:

On behalf of the Executive Committee and the Board of Directors of Marshfield Clinic, I am writing to respond to questions from Ranking Member Camp in follow-up to the hearing on promoting the adoption and use of health technology, which took place on July 24, 2008.

We appreciate the opportunity to provide our testimony and the following responses to the questions posed by Representative Camp.

Sincerely,

DOUGLAS J. REDING, M.D.
Vice President, Marshfield Clinic
Chairperson Government Relations

1. I understand that you have had a chance to review the health IT bill I introduced last month. Are there provisions in my bill that you believe should become law?

We have reviewed legislation introduced by Rep. Camp, HR 6179. There are several provisions of this legislation that we believe are important:

Section 101 would codify the Office of the National Coordinator for Health Information Technology, we believe this is essential to maintain the continuity of operations begun by Dr. David Brailer and now directed by Dr. Robert Kolodner. In particular, as a vendor of CattailsMD, the CCHIT certified proprietary electronic medical record developed by Marshfield Clinic, we believe that certification is an essential guarantee in an uncertain market that electronic medical records can be relied upon by providers and their patients.

Section 302 eliminates the Sunset applicable to the Stark exception for electronic health records. As we noted in our testimony submitted for the record, Marshfield Clinic is very closely associated with the Ministry Health System as well as other providers serving patients in our service areas. The exception provides some comfort to providers who are wary of any implication of improper referral influences.

Section 303 promotes the expansion of telehealth services. Marshfield Clinic is one of the largest telehealth providers in the country, serving a largely rural population with needs that stretch across state borders. We appreciate the reciprocity provisions and the expansion of telehealth sites of origin, which have been shown to add very minimal expense, and substantially improved access.

Finally, in Section 304 HR 6179 establishes an electronic health demonstration in Federally Qualified Health Centers. Marshfield Clinic is the sponsor of an FQHC known as the Family Health Center in Marshfield, which is nationally distinguished because it provides dental services to the indigent throughout the State of Wisconsin and incorporates periodontal records with the Marshfield Clinic electronic medical record. FQHCs should be supported because they bring us one step closer to the universal health coverage that we believe is necessary, at a reasonable cost.

2. I understand that the Marshfield Clinic is just one of many hospital, clinic, and physician groups that have expressed their concerns about the privacy language in H.R. 6357. What impact do you feel this language would have on your clinic's ability to implement care and quality improvement programs as well as to monitor and prevent fraud?

We are concerned that HR 6357, the "Protecting Records, Optimizing Treatment and Easing Communications through Health Care Technology Act of 2008" will increase the costs of providing health care and the cost of implementing electronic medical records without any measurement of the problem it is trying to solve. Provisions of HR 6357 may interfere with activities defined as "operations" under HIPAA that are essential to effective care management.

As we stated in our testimony, to improve quality performance, the Clinic developed software systems to care for chronically ill patients, to identify improvement opportunities, collect needed information at the point of care, and report performance back to physicians.

For example, our PreServ (Preventive Services) System is able to alert physicians when preventative services are due for a patient during a visit with a primary care manager.

Our EMR also includes a system for flagging high-priority patients. A "hierarchical defect recovery list," which acts as a safety net, includes high-risk patients with multiple chronic conditions that are in need of immediate attention.

We have also implemented an anticoagulation care management system for patients on Warfarin.

The Clinic has also implemented electronic prescribing to enhance safety.

We have implemented a 24-hour nurse line, with an automated e-mail system that notifies physicians whose patients have called.

We have developed a software tool called "iList" (Intervention List), which is used in primary care. iList generates a list of patients who have one of three chronic illnesses – diabetes, heart failure or hypertension – and who do not meet all of their recommended health goals.

The PROTECHT Act requires covered entities to make a reasonable effort to restrict the use, disclosure, or request of PHI to a "limited data set" of information as defined in regulation. The PROTECHT Act also includes a new consent provision that requires additional patient consent if the PHI is utilized in operations, such as peer review, quality review, standard of care review, malpractice review, or best practices analysis. We believe that most of our care management processes fall within the definition of the term operations. These activities are the substance of care management, and interference with them interferes with the practice of evidence-based medicine.

In addition, requiring an accounting of disclosures for all disclosures of PHI, including for treatment, payment, and healthcare operations will be difficult. These disclosures are not logged or accounted for - as the law does not currently require this. A requirement to log all these disclosures could add 10 – 30% to the cost of implementing a robust EMR.

How these provisions relate to our effort to prevent fraud.

The Marshfield Clinic electronic medical record includes features that enable us to require authentication for electronic signature of documents and prescriptions. We also use our electronic medical records to facility chart review for coding and other compliance issues.

The electronic medical record includes information about all of the treatments, procedures, diagnostics and therapies provided to any patient. At Marshfield Clinic we utilize the record to assure that patients receive the care that they need when they need it. CMS has shown that this pattern of practice may lead to improved quality of care and substantial savings for the Medicare program.

We refer you to the most recent results of the Physician Group Practice Demonstration, released by CMS August 14, 2008. As a result of improved quality and efficiency made possible through the use of our HIT system in this demonstration Marshfield Clinic will receive a payment from CMS of \$5.78 million as a result of saving the Medicare Trust Funds \$7,226,966 as measured by CMS, under the terms and conditions of the project.

Just as the EMR can be a tool for increasing efficiency, it might also serve as a tool for identifying inefficiencies or intentional over-utilization of services. The EMR also has the potential to serve as an audit tool that could throw light on the diminishing utility of unnecessary, redundant or equivocal services. The problem that Congress must grapple with is that these features of an efficient HIT system may scare some providers away from implementing HIT operational care infrastructure that could retain evidence of wrongdoing. HR 6357 doesn't solve this problem – it makes it less likely that providers could perform operations related to their treatment of patients that would leave an audit trail. We believe that the audit trail and the resulting accountability are in the public interest.

3. Do you feel the current HIPAA protections sufficiently guard patient privacy as it relates to electronic records?

Congress will have to decide where it places its priority. HIPAA is not a perfect law, but it does protect patient privacy. We might also add that electronic medical records are far more secure than paper records or any other alternative. Individual privacy, however, has been utterly compromised because marketing organizations now have many sophisticated tools to track consumer behavior. This information is valuable for marketing goods and services to targeted individuals and populations. To address and deter this invasion into the privacy of individuals, we recommend that congress strengthen enforcement of privacy violations.

What steps does the Marshfield Clinic take to ensure that information found patient's electronic records are kept private and used appropriately?

Marshfield Clinic has put in place the position of Data Security Officer. This is a general manager high-level position reporting directly to the Chief Information Officer of the corporation.

Marshfield Clinic audits all transmissions. For all access we know who accessed data, when and from what device. These audit files are kept indefinitely and can be scrutinized either for random check or for specific cause.

Access to the electronic health record is established within a role-based hierarchy. All employees are assigned a role. Based on the role the employee is only granted access to information necessary to complete their job's functions.

All information is maintained centrally. Information is only delivered to the workstation as a transient "screen shot". No patient data is ever stored remotely on the user workstations.

Education on the importance of security and confidentiality is continuous. All employees are required to annually sign a corporate confidentiality agreement as a term for continuing employment.

The following features complement the security of the Marshfield Clinic EMR:

- Required complexity standards for password authentication.
- Assignment of a primary device, typically a tablet computer for the vast majority of users.
- Security warning to users when they log into a device that is different from the previous device they logged into.
- Role-based security for access to applications.
- Screen designs that avoid casual exposure to patient health data.
- Device locking after a maximum 15 minutes of inactivity on a portable device, and after a maximum of 30 minutes on a tower workstation.
- Document-level audit trails of all user accesses to medical records.
- Review of users' accesses of medical documents for both cause and for sampling of selected users' accesses based on association profile with patients, e.g. co-workers, relatives, or neighbors.
- Routine suppression of health protected on data warehouse reports.
- End user access agreements including our policy on patient privacy that must be reviewed and affirmed yearly.
- Encrypted transmission of wireless data (AES 128 bit)
- Encryption of down-time data base.
- Minimal storage of patient information on end user devices.
- Physical security of main computer rooms.
- Restricted access of programmers to patient data.
- Anti-tamper hardware features of tablet computers.
- Secure disposal of printed reports.
- All computers have centrally managed virus/malware protection per industry best practice standards.

How does the Marshfield Clinic deal with employees who improperly access medical records?

All suspected breaches are investigated by the corporate data security officer and a senior staff attorney from corporate legal services. Marshfield Clinic handles improper employee access through the Clinic's progressive discipline policy, which may include termination. Discipline appropriate for the investigated findings is rendered. Flagrant and malicious breaches usually result in the termination of the offending employee.