U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology

Privacy and Security Tiger Team
Health Information Technology Policy Committee

Consumer Choice Technology Hearing
June 29, 2010
Washington, D.C.

e-MDs
Written Public Testimony
Michael Stearns

Dr. Blumenthal and members of the Office of the National Coordinator for Health Information Technology's Privacy and Security Tiger Team,

We are deeply honored to have been invited to present before you today. I am Dr. Michael Stearns, a physician by training and currently the President and CEO of e-MDs, Inc., an electronic health record (EHR) and practice management software provider. I also serve as President of the Texas e-Health Alliance, a non-profit policy and advocacy body that is, among other activities, examining consumer consent policy issues at the state level.

With me today is Dr. Millican, a family practitioner and e-MDs user who has graciously agreed to take time away from his busy practice to provide a demonstration of how he uses patient privacy related features during patient care.

We greatly appreciate being given the opportunity to share our approaches to managing sensitive patient information. As we will demonstrate, we have tools in our EHR that allow providers with specified privileges to segment information that they deem as sensitive or confidential. This information is either hidden completely or blocked from being viewed in both the internal and exported versions of a given document. Consumers (i.e., patients and their designated representatives) are given the ability to export their Continuity of Care Record (CCR) from the patient portal with or without the information that is specified as confidential.

e-MDs agrees with the conclusions made in the "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis" document created for the ONC by Mellissa Goldstein, JD and Allison Rein, MS. We feel that a great deal of research is needed to determine best practices that will allow for appropriate consumer controls of protected health information. In our opinion, the policies that evolve around these challenging areas will need to take into consideration the impact on workflow, the level of consumer demand, patient safety issues, administrative requirements, local policies/requirements, and significant educational and technical challenges surrounding the successful implementation of consumer consent mechanisms. We anticipate that the level of consumer interest in having control over

health information will become much greater as HIEs take on a greater role in healthcare. For this reason we are very motivated to contribute to efforts to move these policies forward in a way that protects each consumer's right to confidentiality without compromising patient safety or the appropriate use of health care data for research, efficacy of current therapies, biosurveillance, and public health.

Dr. Millican and I will provide the demonstration and share how the tools are used during patient care. An explanation of these features is provided below along with a response to each of the 11 questions we have been asked to address.

1) ***Describe how the technology implements the patient's consent and the granular choices given to the patient.***
    1. Information can be marked as confidential in several areas of the e-MDs EHR including the Health Summary and Progress Notes sections. Confidential information can also be removed or blocked from view in documents that are exported from the system.
        1. Health Summary views in the EHR: The EHR allows the provider to make components of the health summary (e.g., problems, allergies, medications, past medical history, social history, family history, etc.) confidential and thus viewable only by certain individuals based on their privileges. Protected information can be marked as private "on the fly" while documenting or preselected as confidential during the template development and editing process. The patient does not have a direct role but can ask the provider to mark certain information as confidential. Confidential information is blocked out when viewed by someone who does not have the specified privilege (Figure 1.). For medications a label informs the user that the patient has been prescribed a confidential medication (Figure 2.).

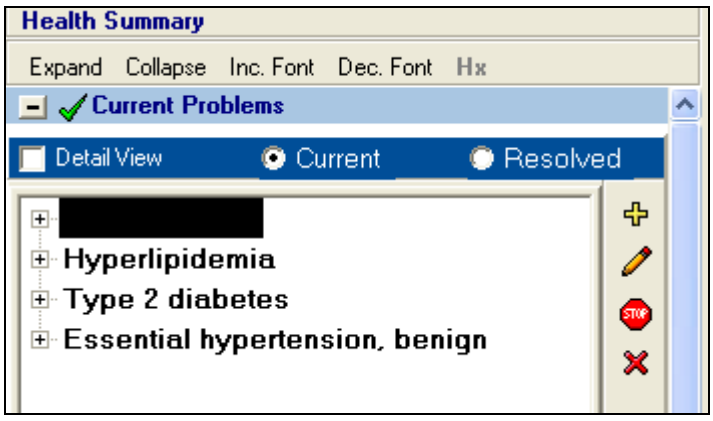

Figure 1. HIV Disease status blocked out

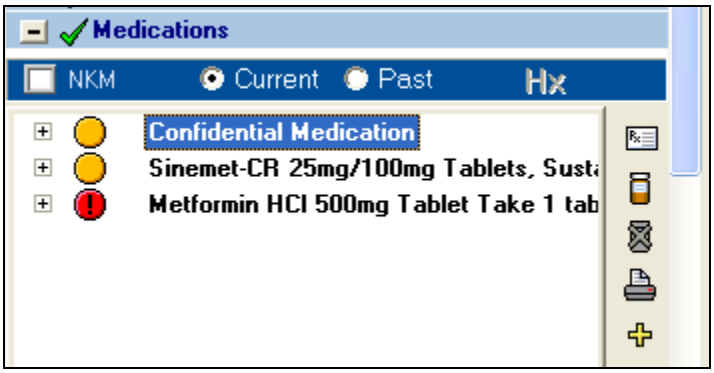

Figure 2. A confidential medication (e.g., an HIV related medication) is displayed as "confidential."

2. EHR Progress Note: Confidential information can be displayed or blocked from view in the progress note as demonstrated in Figures 3 and 4. The printed document will have the same appearance, i.e., the provider will be aware that there is additional information.

SUBJECTIVE:

CC: ◦

Mr. Dynamite is a 70-year-old Caucasian male. ◦ Medical problems to be addressed today include HIV disease. ◦

HPI: ◦

Human Immunodeficiency Virus (HIV) disease ◦

Mr. Dynamite presents with human Immunodeficiency Virus (HIV) disease. ◦ Mr. Dynamite has active AIDS. ◦ This was confirmed 6 months ago. ◦ This diagnosis was made during an office visit at another clinic. ◦ There are no associated symptoms. ◦ Current meds include Fuzeon (enfuviritide) and Lamivudine/Zidovudine. ◦

*Figure 3. Chief Complaint and HPI **without** blocking of confidential information.*

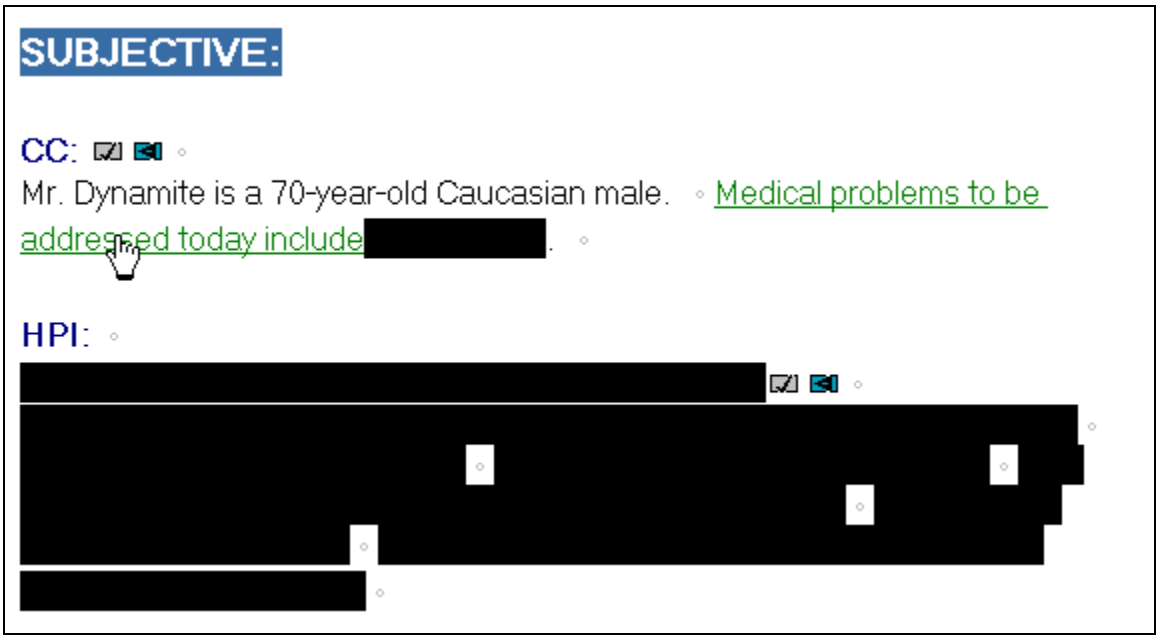

*Figure 4. Chief Complaint and HPI **with** blocking of confidential information.*

3. Exporting and Printing Information:
    1. The provider has the option of printing two versions of the health summary, one with the confidential information and another that removes it from the printed document. In other words, the confidential information does not appear as information that is blocked, but rather it does not appear at all.
    2. Providers using the CCR export feature (and soon the CCD export feature) can export the CCR with or without information marked as confidential.

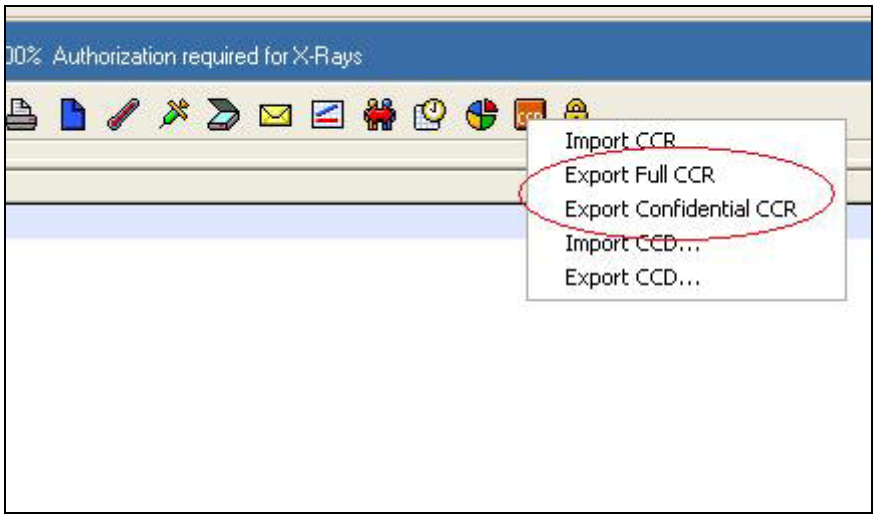

Figure 5. CCR Export Options

3. Patients do have control over what is exported from the e-MDs Patient Portal. When the CCR export utility is used, the patient has the option of exporting their CCR from the patient portal with or without confidential information. This requires, however, that the provider has labeled the information in advance as confidential. However, as patients can see the information in their CCR, they can request that certain items be labeled as confidential via portal communications.

2) How did your system adopt the approach it has taken to patient consent and what was the motivation for doing so?

1. In order to provide the highest quality of care clinicians need to be able to freely document information that may be of a highly sensitive nature, such as mental health issues, chronic illnesses, social history (including but limited to a history of substance use/abuse), certain communicable diseases and other findings that may be considered sensitive. At the core of the provider-patient relationship is an understanding that information shared by the patient will not be used in a manner that could be deleterious to the patient such as their ability to be employed, eligibility for health insurance, and in general social situations. There is a fundamental need to limit, when appropriate, the type of information that is shared by the multitude of stakeholders involved with the clinical, technical and administrative aspects of healthcare.
2. The development and maturation of the e-MDs EHR was initiated over 15 years ago in a multi-provider primary care facility and software development facility where there were extensive interactions between providers, software design specialist and programmers. Early on the need to protect certain sensitive information, allowing it to be restricted as viewable on a need-to-know basis was identified by the clinicians. This lead to several iterations of the confidentiality features described above. This continues to be an ongoing process and the advent of health information exchanges will further increase the priority level of confidentiality tools.

3) How long has the technology been in use?

1. The initial confidentiality tools were released in 2005.

4) How do the providers who use your system handle granular consent? Does it alter the way they view a patient's health record when they receive it?

1. Providers in the same facility with the appropriate privileges can unblock the protected information by making one click on a "Confidentiality Switch." Once the document with the information blocked is exported from a given facility, the blocked content cannot be viewed by other providers. They are provided, however, with an indication in the progress note that the record contains confidential information in the form of an area of the

record that is blocked. This alerts providers to the presence of additional information but it becomes the patient's choice as to whether to share it with this provider. This in many ways mimics the current documentation process whereby providers may elect to not include certain sensitive items in handwritten or dictated documents. Patients may also elect to not share information with their providers. This model informs the providers that there is additional information available, which was done primarily from a patient safety perspective. However, we are open to adjusting this process as further policy regarding the levels of protection of sensitive information in EHRs and HIEs becomes more established.

5) ***What are the advantages to your approach to obtaining patient consent?***
    1. In the "pre-HIE" era, there was less demand on providers, patients, administrators, policy makers, and the HIT industry to provide tools that allow for segmentation of sensitive information in the EHR and related data repositories. Policies, workflow and technology issues related to the protection of confidential information in the digital era are areas of vigorous debate with the U.S. healthcare system. We see our tools as being one early and partial approach to meeting the needs of patients, provides and other healthcare stakeholders. The advantage of this process is that the providers have tools that allow them to serve as patient advocates. The patient have some ability to decide what information is shared via what they export from their patient portal, however, additional patient centric controls are needed.
6) ***Is the technology scalable so that small and medium-sized providers could implement it?***
    1. This technology was designed for all providers regardless of practice size and is available to all of our current users.
7) ***Is the consent technology interoperable with other systems? (i.e., can the patient's consent preferences be passed to other systems within an HIE?)***
    1. At this point the segmented privacy information is not available to external facilities or HIEs. As part of our roadmap we would like to participate in research that identifies the best practices, optimal workflows, patient centric tools, and technologies that allow for an adequate level of granular consent management at both the patient and provider levels.
8) ***If the consent is not interoperable, what technological change would be needed to make it interoperable?***
    1. Information captured as structured data could be marked as protected information (e.g., through an attribution relationship or other method) that could be shared with other systems, however to be truly interoperable this would require standards that were embraced by the industry or required from regulatory bodies.
9) ***What resources are necessary to implement the consent system in its current form? What further resources would be necessary to offer increased granular consent choices?***
    1. The consent system in its current form is an integral part of our EHR and is available to all of our current users. Additional training, in particular

when these tools become more essential once HIEs become more entrenched, will be needed to keep our customers fully informed regarding patient consent issues.

10) How many systems or users are currently implementing or adopting this technology?

1. While this feature is available to thousands of e-MDs' users, the majority of their documentation is not shared outside of their facility (with the exception of billing codes). As HIEs become more ubiquitous in our society, sharing of sensitive information in digital formats will likely become a much greater concern to patients and providers. We anticipate that the usage of our current tools and demand for additional consumer choice features will grow significantly.

11) How many unique consumers are covered by the technology that is implementing the consumer choice system?

1. e-MDs has over 27,000 users in 49 states and U.S. territories. All told this technology could impact well over 1,000,000 patients served by our providers. However, the technology described above is not used by the majority of our providers as it is not currently viewed as essential to providing care at the facility level. We anticipate this could change significantly over the next 24 months as interoperability becomes a point of emphasis in the health care industry.

Sincerely,

Michael Stearns, MD
President and CEO, e-MDs, Inc.
9900 Spectrum Drive
Austin, Texas 78717
Author and copresenter

Troy Millican, MD
2122 HWY 71 South
Columbus, Texas 78934
Copresenter