SITH-II Panel: Clinical Systems---Have Access Control Methodologies Kept Pace?

May 15th, 2012
• Who am I?
  – Degree of certainty
• How long am I Present?
  – Timeouts
  – Proximity
  – Partial re-authentication
• Real world challenges....
  – the data and the panel
The “Access Control Hygiene” Problem

Professor Andy Gettinger, Geisel School of Medicine; Professor Sean Smith, Computer Science
Definition: Authentication Factors

• Factor: something you know
  – Example: User name & password

• Factor: something you have
  – Example: Token (physical or electronic)

• Factor: something you are
  – Example: Biometric: voice, facial recognition, iris scan, finger print
### Meaningful Use Stage One

**No Requirement for Specific or Multiple Authentication Factors**

<table>
<thead>
<tr>
<th>Meaningful use Stage 1 objective</th>
<th>Meaningful use Stage 1 measure</th>
<th>Certification criterion</th>
</tr>
</thead>
</table>
| Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. | Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process. | Interim Final Rule Text: 
(1) Local. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.
(2) Cross network. Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in § 170.210(d).

Final Rule Text: § 170.302(l). Authentication. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. |

**Comments:** One commenter expressly supported this certification criterion. A majority of commentators expressed concerns related to § 170.302(l) and the cross-enterprise authentication standard specified at § 170.210(d). Some commentators misinterpreted our example and stated that Security Assertion Markup Language (SAML) should not be required or be a named standard. One commenter suggested expanding the set of examples we provided. Other commentators requested that the standard and the related portion of the certification criterion be removed because it was too burdensome to implement at the present time, was overly broad, and could be subject to multiple interpretations. Other commentators insisted that there is an insufficient infrastructure to support cross-enterprise authentication. One commenter stated that cross-enterprise authentication would not reside in an EHR application, but rather in the network infrastructure.

Response. We have considered the concerns issued by commentators and agree that the burden associated with cross-enterprise authentication is unnecessarily high and cross-network authentication should not be a condition of certification at the present time. As a result, we have removed this specific part of the certification criterion and the associated standard.

**Comment:** A commenter requested clarification as to whether “user name and password” would be sufficient to authorize a user or whether biometrics would be required.

Response. We do not believe that it is appropriate to specify, as a condition of certification, the types of factors that users could utilize to authenticate themselves.

---

**Professor Andy Gettinger, Geisel School of Medicine; Professor Sean Smith, Computer Science**
DOJ: Multiple Factor Authentication Required by the DEA

DEPARTMENT OF JUSTICE
Drug Enforcement Administration
21 CFR Parts 1300, 1304, 1306, and 1311
[Docket No. DEA–2181]
RIN 1117-AA61

Electronic Prescriptions for Controlled Substances

AGENCY: Drug Enforcement Administration (DEA), Department of Justice.

ACTION: Interim Final Rule with Request for Comment.

SUMMARY: The Drug Enforcement Administration (DEA) is revising its regulations to provide practitioners with the option of writing prescriptions for controlled substances electronically. The regulations will also permit pharmacies to receive, dispense, and archive these electronic prescriptions. These regulations are in addition to, not a replacement of, the existing rules. The regulations provide pharmacies, hospitals, and practitioners with the

2010. Commenters should be aware that the electronic Federal Docket Management System will not accept comments after Midnight Eastern Time on the last day of the comment period. ADDRESSES: To ensure proper handling of comments, please reference “Docket No. DEA–218” on all written and electronic correspondence. Written comments sent via regular or express mail should be sent to the Drug Enforcement Administration, Attention: DEA Federal Register Representative/ODL, 8701 Morrissette Drive, Springfield, VA 22152. Comments may be sent to DEA by sending an electronic message to dea.diversion.policy@usdoj.gov. Comments may also be sent electronically through http://www.regulations.gov using the electronic comment form provided on that site. An electronic copy of this document is also available at the http://www.regulations.gov Web site. DEA will accept attachments to electronic comments in Microsoft Word, WordPerfect, Adobe PDF, or Excel file formats only. DEA will not accept any file formats other than those specifically

Administration’s public docket. Such information includes personal identifying information (such as your name, address, etc.) voluntarily submitted by the commenter.

If you want to submit personal identifying information (such as your name, address, etc.) as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase “PERSONAL IDENTIFYING INFORMATION” in the first paragraph of your comment. You must also place all the personal identifying information you do not want posted online or made available in the public docket in the first paragraph of your comment and identify what information you want redacted.

If you want to submit confidential business information as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase “CONFIDENTIAL BUSINESS INFORMATION” in the first paragraph of your comment. You must also prominently identify confidential business information to be redacted within the comment. If a comment has
• 48 respondents
  – 3 clinicians, 45 IT professionals
• Method to authenticate
  – 95% use passwords
  – 4% use 4 digit pin
  – 13% (three sites) additional factor
### What rules are placed on the character set of passwords?

<table>
<thead>
<tr>
<th>Rule</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only lowercase letters</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Upper and lowercase letters</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Alphanumeric</td>
<td>13.6%</td>
<td>3</td>
</tr>
<tr>
<td>Alphanumeric and non-alphanumeric symbols</td>
<td>50.0%</td>
<td>11</td>
</tr>
<tr>
<td>No such rules</td>
<td>27.3%</td>
<td>6</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>9.1%</td>
<td>2</td>
</tr>
</tbody>
</table>

Answered question: 22
Skipped question: 26
<table>
<thead>
<tr>
<th>Frequency</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than once a month</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Monthly</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Every 3 months</td>
<td>54.5%</td>
<td>12</td>
</tr>
<tr>
<td>Every 6 months</td>
<td>31.8%</td>
<td>7</td>
</tr>
<tr>
<td>Annually or longer</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>No such restrictions</td>
<td>9.1%</td>
<td>2</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>4.5%</td>
<td>1</td>
</tr>
</tbody>
</table>

| answered question | 22 |
## Use of Second Factor Rare

### 28. Does your EMR system use a possession-based authentication technique?

<table>
<thead>
<tr>
<th>Response</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>9.4%</td>
<td>3</td>
</tr>
<tr>
<td>No</td>
<td>90.6%</td>
<td>29</td>
</tr>
</tbody>
</table>

Answered question: 32
Skipped question: 16

### 29. Which of the following possession-based authentication techniques do you employ?

<table>
<thead>
<tr>
<th>Technique</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Smartcard</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>USB token</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Any device requiring the user to input a code generated on the device (for example, RSA SecurID)</td>
<td>66.7%</td>
<td>2</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>66.7%</td>
<td>2</td>
</tr>
</tbody>
</table>

Answered question: 3
Skipped question: 45

---

Professor Andy Gettinger, Geisel School of Medicine; Professor Sean Smith, Computer Science
### Is continuous contact between the token and reader required to remain authenticated?

<table>
<thead>
<tr>
<th>Response</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>No</td>
<td>100.0%</td>
<td>3</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>0.0%</td>
<td>0</td>
</tr>
</tbody>
</table>

answered question: 3
skipped question: 45

### Is it used in conjunction with knowledge-based authentication?

<table>
<thead>
<tr>
<th>Response</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>66.7%</td>
<td>2</td>
</tr>
<tr>
<td>No</td>
<td>33.3%</td>
<td>1</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>0.0%</td>
<td>0</td>
</tr>
</tbody>
</table>

answered question: 3
skipped question: 45
### Does your EMR system use a biometric-based authentication technique?

<table>
<thead>
<tr>
<th></th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>6.3%</td>
<td>2</td>
</tr>
<tr>
<td>No</td>
<td>93.8%</td>
<td>30</td>
</tr>
</tbody>
</table>

answered question 32
skipped question 16

### 45. Have any individuals refused to use biometric authentication, citing concerns about the privacy or security of their biometric data?

<table>
<thead>
<tr>
<th></th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>100.0%</td>
<td>2</td>
</tr>
<tr>
<td>No</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>0.0%</td>
<td>0</td>
</tr>
</tbody>
</table>

answered question 2
skipped question 46

Professor Andy Gettinger, Geisel School of Medicine; Professor Sean Smith, Computer Science
### De-authentication Time-outs

#### How long is the timer?

<table>
<thead>
<tr>
<th>Duration</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 minutes</td>
<td>11.1%</td>
<td>2</td>
</tr>
<tr>
<td>15 minutes</td>
<td>50.0%</td>
<td>9</td>
</tr>
<tr>
<td>30 minutes</td>
<td>16.7%</td>
<td>3</td>
</tr>
<tr>
<td>1 hour</td>
<td>11.1%</td>
<td>2</td>
</tr>
<tr>
<td>greater than 1 hour</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>11.1%</td>
<td>2</td>
</tr>
</tbody>
</table>

- **Answered question**: 18
- **Skipped question**: 30

---

Professor Andy Gettinger, Geisel School of Medicine; Professor Sean Smith, Computer Science
“State of the art” as practiced in four large and well-known academic settings

– University of California San Diego
– Yale
– Penn
– Dartmouth