Data Information Systems Infrastructure: Critical Standards and Best-Practices

Executive Summary

MICYRN's Clinical Research Informatics Initiative brings together a collegiate group of knowledge experts from MICYRN Member Research Institutes and affiliated research networks to provide input and advice on the development of a national clinical research informatics platform. One of the emergent needs expressed across the group has been the development of quality standards for clinical research information systems across the network. The growth of REDCap installation and use for research studies has heightened this requirement; moreover, the validated MICYRN instance of REDCap which has been implemented to support regulated studies, has provided further impetus to arrive at a common set of system best-practices and standards.

The UK Clinical Research Collaboration has conducted much work in the area of system standards, having initiated a Data Information and Management Systems (DIMS) project in 2008. The result of the project is a set of recommendations around the development of a number of functional and operational standards in support of trials unit information systems.

The white paper can be accessed publicly at: http://www.ukcrc.org/infrastructure/ctu/activitiesassociatedwithctu/

Using the critical standards and best practices from the UKCRC work as a starting point, the CRI Core was surveyed as to whether they met and then whether they agreed to each of the UKCRC standards. The results of the survey were subsequently reviewed with the group over a series of teleconferences; as part of the review, decisions were made as to whether the MICYRN network should accept, revise or reject each standard with an aim to arrive at a minimum quality standard for the MICYRN REDCap Instance.

What follow are the results of the CRI Core group recommendations on critical standards (“must-haves”) and best-practices (“should-haves”) for Research Information Systems Infrastructure across the MICYRN Network – these quality standards become the minimal infrastructure standards for the MICYRN REDCap Instance, but also serve as a reference for other systems across or within MICYRN Research Institutes. Subsequent work of the group on standards will be in the areas of system/environment information security and system functionality.
## Definitions

Critical Standard – Important, often fairly basic standards of operation that are reasonably attainable and must therefore be implemented, at minimum, if an information system is to be considered “high quality”.

Best-Practice – Practices that should be implemented if an information system is to be considered “high-quality”, assuming they are applicable to the operation of the system.

## Results

### (1) Procurement & Installation (Servers)

<table>
<thead>
<tr>
<th>(a) Best-Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. <strong>Specification</strong>: Servers and similar equipment should be specified and selected according to the specific requirements of the trials unit and the functions being supported</td>
</tr>
<tr>
<td>ii. <strong>Purchasing</strong>: Purchases should comply with policies stipulated by the host organization or show evidence of appropriate selection between alternate suppliers</td>
</tr>
<tr>
<td>iii. <strong>Installation and Build</strong>: Detailed records of builds must be available, for maintenance and safe rebuilding</td>
</tr>
</tbody>
</table>

### (2) Physical Access Control (Servers and Admin Server Desktop Consoles)

<table>
<thead>
<tr>
<th>(a) Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. <strong>Servers</strong>: Servers must be housed within a dedicated locked room with unescorted access limited to specified individuals</td>
</tr>
<tr>
<td>ii. <strong>Desktops</strong>: Admin Server Desktop Consoles that hold or access server administration data - should be located in locked room(s) with restricted access (e.g. by key code, swipe card)</td>
</tr>
</tbody>
</table>

### (3) Area Management (Servers)

<table>
<thead>
<tr>
<th>(a) Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. <strong>Power Supply</strong>: The power supply to critical production servers should be secured, e.g. by a UPS unit or secondary generator</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(b) Best-Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. <strong>Maintenance</strong>: Necessary server patches and updates should be applied in a timely but safe manner to: a) The operating system b) Anti-malware systems c) Backup systems d) Major apps (e.g. SQL Server, Citrix, Clinical DBMSs, etc.)</td>
</tr>
<tr>
<td>ii. <strong>Hazard Control</strong>: The server room should be fitted with heat and smoke alarms, monitored 24/7</td>
</tr>
</tbody>
</table>

### (4) Logical Access Control (Servers & Networks)

<table>
<thead>
<tr>
<th>(a) Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. <strong>Admin role</strong>: Servers should be protected by a highly restricted administrator password (i.e. known to essential systems staff only)</td>
</tr>
<tr>
<td>ii. <strong>Access rights</strong>: Users should only have the minimum necessary access to carry out their roles</td>
</tr>
<tr>
<td>iii. <strong>Firewalls</strong>: External firewalls should be in place and configured to block inappropriate access</td>
</tr>
<tr>
<td>iv. <strong>Access Rights</strong>: Users roles and rights should be reviewed and amended regularly to reflect changes</td>
</tr>
<tr>
<td>v. <strong>Network password management</strong>: Should be enforced on all users, including regular password change and password complexity</td>
</tr>
<tr>
<td>vi. <strong>Access Rights</strong>: Access control for any remote access (e.g. via Citrix) controlled to the minimum required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(b) Best-Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. <strong>Testing</strong>: Regular penetration testing by host organization should occur, at least 6 monthly, with appropriate responses</td>
</tr>
</tbody>
</table>

### (5) Business Continuity

<table>
<thead>
<tr>
<th>(a) Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. <strong>Business Continuity</strong>: A basic BC plan should be present, covering likely action in event of possible</td>
</tr>
</tbody>
</table>
disasters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ii.</td>
<td><strong>Back up:</strong> Documents detailing backup policy, procedures, restores and testing must be in place</td>
</tr>
<tr>
<td>iii.</td>
<td><strong>Back up:</strong> Back ups must be taken at least nightly, using a managed, documented regime</td>
</tr>
<tr>
<td>iv.</td>
<td><strong>Back up:</strong> Back ups should be stored in a secure environment offsite or a secured and fireproof environment if onsite</td>
</tr>
<tr>
<td>v.</td>
<td><strong>Recovery:</strong> Testing of full restore procedures should take place at least annually</td>
</tr>
</tbody>
</table>

#### (b) Best-Practice

| i. | **Business Continuity:** A detailed plan should be present covering specifics of actions, contacts, suppliers, etc. |
| ii. | **Business Continuity:** The detailed plan should be integrated with the host organization's BC plan and appropriate access |
| iii. | **Business Continuity:** Regular review, should occur, at least annually, of the detailed BC plan |

#### (6) In House Software Development

##### (a) Critical

| i. | **Procedures:** SOPs / policies should exist on in-house development, including risk assessment |

##### (b) Best-Practice

| i. | **Specification:** A functional spec. should be available, e.g. use cases, according to procedures |
| ii. | **Documentation:** Adequate documentation should exist, e.g. for components, architecture, functions, calls, etc. |
| iii. | **Source Control:** Source code versions should be maintained (if only via standard backup) |

#### (7) Validation (General)

##### (a) Critical

| i. | **Procedures:** SOPs / policies should be in place on system validation, including risk assessment |
| ii. | **Planning:** Validation plans should be drawn up for any particular system, listing extent / types of tests |
| iii. | **Testing:** Testing should be carried out and recorded, normally against requirements and / or validation plan |

#### (8) User Training & Support

##### (a) Critical

| i. | **IS Support:** Mechanism(s) for requesting support should be in place |
| ii. | **IS Support:** Help and related materials should be available for users |

##### (b) Best-Practice

| i. | **Policies:** Policies / SOPs should be in place describing induction and training requirements / policies / procedures |
| ii. | **Core training:** Induction / Training and regular update must include (a) GCP (b) Data Protection (c) Record Confidentiality |
| iii. | **Records:** Records of Training should be in place for all staff, held centrally and / or by the staff themselves |
| iv. | **IS Training:** Users of systems must be adequately trained (may not be formal training) |
| v. | **IS Support:** External users should also be supported where they exist |

#### (9) IT Staff Competence

##### (a) Critical

| i. | **Compentence:** Staff should be previously competent, trained or being trained to do the job(s) required of them |

##### (b) Best-Practice

| i. | **Records:** Record of technical training / competence should be in place for IT staff |

#### (10) General Quality Management System (QMS) Integration

##### (a) Best-Practice

| i. | **QMS Docs:** QMS Documentation should be up-to-date, well organized, indexed and readily available |
| ii. | **QMS Procedures:** Policies / procedures should be documented, reflect good practice and be used in |
iii. **Integration**: IT Standards documents and systems should be integrated with the overall QMS
iv. **Training**: Staff members should be trained on relevant policies and procedures
v. **QA Review**: Policies and procedures should be regularly reviewed
vi. **QA Processes**: QA Procedures should exist covering the writing, review and approval of QA documents, e.g. SOPs
<table>
<thead>
<tr>
<th>MICYRN Members</th>
<th>First</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFRI</td>
<td>British Columbia</td>
<td>Victor Espinosa</td>
</tr>
<tr>
<td>ACHRI</td>
<td>Calgary</td>
<td></td>
</tr>
<tr>
<td>WCHRI</td>
<td>Edmonton</td>
<td>Lawrence Richer</td>
</tr>
<tr>
<td></td>
<td>Edmonton</td>
<td>Rick Watts</td>
</tr>
<tr>
<td></td>
<td>Edmonton</td>
<td>Pam Marples</td>
</tr>
<tr>
<td>U.Sask</td>
<td>Saskatoon</td>
<td></td>
</tr>
<tr>
<td>MITCH</td>
<td>Winnipeg</td>
<td>Susan Acland</td>
</tr>
<tr>
<td></td>
<td>Winnipeg</td>
<td>Daniel Despins</td>
</tr>
<tr>
<td></td>
<td>Winnipeg</td>
<td>Steve Nesbitt</td>
</tr>
<tr>
<td>Laurentian</td>
<td>Sudbury</td>
<td>Nancy Young</td>
</tr>
<tr>
<td>Queens</td>
<td>Kingston</td>
<td>Lucia Ruhland</td>
</tr>
<tr>
<td></td>
<td>Kingston</td>
<td>Helen Coo</td>
</tr>
<tr>
<td>CHRI</td>
<td>London</td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>Hamilton</td>
<td>Lindsay Akrong</td>
</tr>
<tr>
<td>MtSinai</td>
<td>Toronto</td>
<td>Nida Shahid</td>
</tr>
<tr>
<td>Sunnybrook</td>
<td>Toronto</td>
<td></td>
</tr>
<tr>
<td>Sick Kids</td>
<td>Toronto</td>
<td>Christopher Battiston</td>
</tr>
<tr>
<td></td>
<td>Toronto</td>
<td>Wayne Arnold</td>
</tr>
<tr>
<td></td>
<td>Toronto</td>
<td>Rulan Parekh</td>
</tr>
<tr>
<td></td>
<td>Toronto</td>
<td>Tom Walters</td>
</tr>
<tr>
<td></td>
<td>Toronto</td>
<td>Dragan Kljujic</td>
</tr>
<tr>
<td>CHEO</td>
<td>Ottawa</td>
<td>Lisa Nesbitt</td>
</tr>
<tr>
<td></td>
<td>Ottawa</td>
<td>Yael Kamil</td>
</tr>
<tr>
<td>McGill</td>
<td>Montreal</td>
<td>Elise Mok</td>
</tr>
<tr>
<td>St.Justine</td>
<td>Montreal</td>
<td>Benoit Masse</td>
</tr>
<tr>
<td>U.Sherbrooke</td>
<td>Sherbrooke</td>
<td></td>
</tr>
<tr>
<td>U.Laval</td>
<td>Laval</td>
<td></td>
</tr>
<tr>
<td>IWK</td>
<td>Halifax</td>
<td>Marjorie Sullivan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lisa Currie</td>
</tr>
<tr>
<td>Memorial</td>
<td>Newfoundland</td>
<td>Karen Murphy</td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NeuroDevNet</td>
<td>Elodie</td>
<td>Portales-Casamar</td>
</tr>
</tbody>
</table>