ANNEX A

CYBERSECURITY BEST PRACTICES FOR PHMCA LICENSEES

Policy, Governance and Training

1. Cybersecurity should be viewed as a risk management issue, which should be managed by the licensee (or in some cases, the senior management or Board of larger institutions). It should not be viewed merely as a technical or IT issue. This is to ensure decisions are deliberated at the appropriate senior leadership level, to balance the trade-offs between security, operational requirements, and cost.

2. All institutions should ensure that they develop and institute a clearly stated IT security policy and communicate the policy to all relevant employees and staff.

3. All employees and staff in the institution are to be regularly informed of the risks and threats of cyber-attacks and be trained to abide by good cyber hygiene practices. The training should include:

    a. User-security safe practices including use of strong passwords or passphrases, avoid using the same passwords for different applications or Internet online accounts, avoid clicking on unknown web-links and attachments received from emails, and to limit sharing of personal information on social media, to avoid identify theft and impersonation;

    b. Identifying potential cyber incidents, including unusual or suspicious activities on the IT systems, including email phishing attacks, unverified logins, unauthorised accesses to accounts, etc.; and

    c. Timely response to cyber incidents, including the communications and escalation of such incidents for prompt investigations and containment.

4. Ensure that any outsourced IT vendors maintaining their IT systems are familiar with the cyber hygiene measures, including the protection, detection, respond and recovery measures as outlined below.

Protection and Detection Measures

5. Put in place safeguards to protect electronic medical records. For example:

    a. Ensure appropriate anti-virus security software is installed on all personal computers and servers used in the institution and to ensure that these systems are regularly updated and functioning in a proper manner.

    b. Ensure management of software patches is conducted in a timely and rigorous manner to reduce vulnerabilities to any cyber-attacks;

    c. Only permit authorised software to be installed on the institutions' personal computers and servers;

d. Use strong passwords;

e. Ensure that users are only given access to information that is relevant and necessary for the roles that they perform;

f. Conduct ad-hoc audits on the user and system activities within personal computers and servers to detect unauthorised activities and accesses;

g. Restrict the use of personal removable storage devices on the institutions' IT systems and personal computers, wherever possible. This should be implemented through technical controls where practical

h. Ensure that all personal information on storage media (including portable hard drives and removable storage media) are securely deleted, erased or destroyed before redeploying, exchanging or disposing of the media.

i. As far as is practicable, limit Internet access from workstations that have access to electronic medical records to only what is critical for official work purposes.

6. Some licensees may have systems with "privileged accounts". These are user accounts with additional privileges which enable the users to manage the IT systems and data within the institution. The impact of a compromised "privileged account" is significant. Hence, all licensees should institute the following measures for such "privileged accounts", unless there is a valid justification:

    a. Protect such privileged accounts against unauthorised access by using 2FA two-factor authentication systems;

    b. The use of passphrases for added security;

    c. Sharing of passwords to be disallowed; and

    d. Audit and investigate unauthorised attempts to access or suspicious events involving privileged accounts.

7. For healthcare institutions with significant amount of electronic health records, licensees are encouraged to explore and implement additional security solutions, where appropriate. Some examples that could be considered include:

    - Advanced malware detection tools;
    - Anti-spyware systems;
    - Encryption software to protect the confidentiality of patient data;
    - Firewalls to be deployed to protect the institution's network from Internet attacks;
    - Intrusion prevention/detection systems; and
    - Web proxy servers.

Respond and Recovery Measures

8. Periodically perform system and data backups, with such backups kept securely offline, to prevent unauthorised access and to facilitate recovery in the event of a cyber- incident.

9. Develop and maintain a proper response plan to cyber incidents, including the communications and escalation of such incidents to the appropriate party within the institution for prompt investigations. Where appropriate, institutions should conduct cybersecurity exercises to familiarise its employees and staff on such response plans.

10. Where appropriate, consider engaging IT security service providers to provide cyber security response and recovery services. These partners can assist in ensuring timely response to cyber-attacks and reduce impact of such cyber-attacks.

----End----