附件五

处理香港电子健康纪录的安全措施守则

1. 信息安全治理	
1.1	机构须要求所有需要处理香港电子健康纪录的员工 (包括 IT 人员)签署保密协议，以保护包括患者纪录在内的机密数据，防止未经授权的使用和泄露。
1.2	建立定期安全审计机制，对使用香港电子健康病历纪录进行审计、事件分析和取证调查（如有必要）。
1.3	禁止所有员工共享使用病历纪录系统的工作站的登录凭证。
1.4	机构需要定期对所有员工传达信息安全要求、进行安全意识培训。
1.5	下载香港电子健康病历纪录需要在 60 天内删除，香港医务卫生局保留进行审计相关纪录的权利。
2. 系统安全 ,数据加密, 网络安全和物理上的保护要求	
2.1	所有员工都需要使用凭证（用户 ID 和密码）登入处理香港电子健康纪录的系统的工作站。
2.2	有关工作站在无人值守（例如闲置 20 分钟后）时，启用了带有密码保护的屏幕保护程序。
2.3	下载香港电子健康病历纪录必须加密存储和有适当的物理保护。对于对称加密，至少应采用 256 位 AES 或同等协议。对于非对称加密，至少应采用 2048 位 RSA 或等效算法。
2.4	必须定期对使用香港电子健康病历纪录的系统/工作站进行网络漏洞，系统安全评估，并及时修复任何安全漏洞。
2.5	所有系统账户密码都需要启用强密码。 （以下是香港政府资讯科技总监办公室的强密码政策，以作参考: ➢ 复杂性和长度：至少八个字符，包含大写英文字母、小写英文字母、数字和特殊字符；或至少包含三个类别的十个字符 ➢ 密码历史：记住至少 8 个密码

	➢ 帐户锁定：五次或更少的无效登录尝试后 ➢ 定期修改密码：每六个月或更频繁）
2.6	有流程确保操作系统软件和浏览器软件应用最新的安全更新，并确保及时为所有用于使用香港电子健康病历纪录的系统/工作站（例如 PC，笔记本电脑等）安装关键安全补丁。
2.7	有流程确保监控、报告和处理信息安全事件和违规行为。
2.8	若发生资讯安全事件，应立即报告给香港医务卫生局及医院管理局。