CAREREVIEW® ndol Mill Rd., Ste. 601
'6011 817-652-9800

Information Security Policy

This document contains information related to security procedures to be established by Provider or medical professional before the Effective Date of the Provider Agreement and maintained throughout the Term. These procedures are in addition to the requirements of the Provider Agreement and present a minimum standard only. However, it is Provider's sole obligation to (i) implement appropriate measures to secure its systems and data, including CareReview, Inc. and its customer's proprietary, confidential, or personal information, including individual health information, that Provider may receive or have access to under the Provider Agreement (collectively, "Proprietary Information"), against internal and external threats and risks; and (ii) continuously review and revise those measures to address ongoing threats and risks. Failure to comply with the minimum standards set forth in this document will constitute a material, non-curable breach of the Provider Agreement by Provider, entitling CareReview, Inc., in addition to and cumulative of all other remedies available to it at law, in equity, or under the Provider Agreement, to immediately terminate the Provider Agreement. Unless specifically defined in this document, capitalized terms will have the meanings set forth in the Provider Agreement.

1. **COMPUTER SYSTEMS CONTROL**
    a. "Computer Systems" means any computer, network or system that is used by Provider or its agents or employees to access, store or process any Proprietary Information.
    b. Provider shall not install illegal, malicious or unlicensed software on its Computer Systems.
    c. Provider must not test or attempt to compromise any information security mechanism put in place by CareReview, Inc.
    d. Restriction against Web Hosting – Provider shall not host any web services from any computer that is used to access CareReview, Inc.'s systems or store or process Proprietary Information.
    e. Email Use – if any Proprietary Information is ever sent over email, the email service used must have opportunistic TLS enabled over SMTP.
    f. Computer Systems must have antivirus software installed and enabled with auto-update enabled.
    g. Computer Systems must have auto-update enabled for security updates.
    h. Computer Systems must have firewall and hard-drive encryption enabled.
    i. Web browsers utilized to access Proprietary Information must be kept current and Provider will not lower the default security level settings.
    j. Passcode – A passcode of a minimum 4 characters must be enabled on all Computer Systems.
    k. Provider will configure their computer systems to require usernames and passcodes, and require that such usernames and passcodes be used only by the person authorized, and not permit any sharing of passcodes or usernames.
    l. Wireless network access must be protected using an authentication and encryption method.

2. **OFFICE SECURITY AND TRAVEL**
    a. Printing. When printing Proprietary Information, only secure printer locations may be used.
    b. When working remotely, Provider must take due care not to leave any Computer Systems unattended.
    c. Provider shall not log into, or attempt to log into, public WiFi using any Computer Systems.

3. **DISPOSAL**
    a. Provider agrees to dispose of all Proprietary Information at termination of contract.
    b. To dispose of data, Provider must permanently wipe Proprietary Information from the Computer Systems' hard drive utilizing a hard drive sanitization tool.

4. **REPORTING INCIDENTS:** All suspected disclosures or suspected compromise of Proprietary Information or any Computer Systems must be reported immediately to CareReview, Inc.

5. **INDEMITY CLAUSE:** Provider will hold CareReview, Inc. harmless from claims, damages, and expenses incurred by CareReview, Inc. resulting from a breach of the Provider's security or any violation of the terms of this document.