Rutland Regional Medical Center Confidentiality and Security Agreement

Rutland Regional Medical Center (RRMC) has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, RRMC must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

I understand that all RRMC workforce members (including but not limited to physicians, employees, students, trainees, volunteers, vendors and others who perform work for RRMC) and authorized users of the RRMC systems are personally responsible for ensuring the privacy and security of all patient, confidential, restricted, and proprietary information to which they are given access to.

Further, I understand that as a user of RRMC information systems I am responsible for accessing and using patient and other confidential information in a manner that is consistent with the Agreement and the needs of RRMC in managing health information as part of its mission to provide integrated health services to those in the Rutland Region and surrounding communities.

In the course of my access to RRMC systems, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the policies of RRMC and/or the entity that I am employed or otherwise affiliated with. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to RRMC Confidential Information or RRMC systems.

General Rules

1. I understand that I should have no expectation of privacy when using RRMC systems. RRMC may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security. In addition, I agree to cooperate with any audit performed by RRMC including providing access to any computer that is used for remote access.
2. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to access the system. I also understand that unauthorized access, misuse, or breach of Confidential Information may constitute a crime or civil violation and I understand that RRMC may be legally obligated to report suspected conduct to one or more governmental agencies.
3. I understand that RRMC may decide at any time without notice to no longer provide access to any systems unless other contracts or agreements state otherwise.

Protecting Confidential Information

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
2. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter.
3. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.
4. I will not make any unauthorized transmissions, inquiries, modifications, or purging of Confidential Information.
5. I will secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with industry-approved security standards, such as encryption.

Following Appropriate Access

1. I understand that access means the ability or means necessary to read, write, modify, or communicate data/information or otherwise make use of any RRMC system resource, and that remote access means the ability to access RRMC systems from a remote location, which includes home office users, non-RRMC facilities, and/or business associates.
2. I will only access or use systems or devices I am officially authorized to access, will only do so for the purpose of delivery of medical services, health care operations, or payment.
3. I will only access systems to review patient records when I have a business need to know, and I have the necessary patient consent as required by Vermont law. By accessing a patient's record or RRMC information, I am affirmatively representing

to RRMC at the time of each access that I have the requisite business need to know and appropriate consent, and RRMC may rely on that representation in granting such access to me.

4. I will insure that only appropriate personnel in my office, who have been through a screening process, will access the systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
5. I will accept full responsibility for my actions when I access RRMC systems and Confidential Information.
6. I agree that if I, print or store Confidential Information on non-RRMC media or devices (*e.g*., flash drives, laptops, smart phones) or transmit data by e-mail outside of the RRMC domain, that the data then becomes my sole responsibility to protect according to federal regulations, and I will take full accountability for any data loss or breach.

Doing My Part – Personal Security

1. I understand that RRMC will track my access and use of Confidential Information.
2. I will use a unique identifier to access Confidential Information.
3. I will:
    a. Use only my officially assigned User-ID and password, and if applicable VPN token..
    b. Use only approved licensed software.
    c. Use a device with virus protection software.
4. I will never:
    a. Disclose my password.
    b. Use tools or techniques to break/exploit security measures.
    c. Connect unauthorized systems or devices to RRMC systems.
5. I will practice good workstation security measures such as using screen savers with activated passwords appropriately, and positioning screens away from public view.
6. I will immediately notify RRMC Information Services or my employer if:
    a. my password has been seen, disclosed, or otherwise compromised
    b. media with Confidential Information stored on it has been lost or stolen;
    c. I suspect a virus infection on any RRMC system;
    d. I am aware of any activity that violates this agreement, privacy and security policies; or
    e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or RRMC systems.

Upon Termination

1. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with RRMC.
2. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with RRMC. However, I understand that RRMC will provide access to the medical records I generated or such other information that is necessary for my entities' treatment, payment, or healthcare operations.

Failure to comply with this agreement may result in termination of access to RRMC systems and corrective action including termination from RRMC for employees. Additionally, there may be criminal and civil penalties for inappropriate uses or disclosures of certain protected information.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above. I further agree that a facsimile or scanned image of my signature is the equivalent of the original signature and is fully enforceable.