# Terms and Conditions of Use for Access to Billings Clinic Electronic Medical Record Systems

THIS AGREEMENT ("Agreement") is entered into between Billings Clinic and the individual or entity listed below and sets forth the terms and conditions under which such individual or entity is permitted to obtain "read only" remote access to electronic health records of Billings Clinic.

**DEFINITIONS**

A. Authorized User: A person authorized by Billings Clinic to access the System.

B. Protected Health Information: Any information (whether oral, written, electronic, or recorded in the medical record, in the System or in any other medium) that identifies or can readily be associated with the identity of a patient and relates to the patient's health care. Protected Health Information includes, but is not limited to:

1. Health/clinical information – diagnosis, treatments, test results, prescriptions, etc.

2. Demographic information – name, age, address, phone number, social security number, etc.

3. Appointment information – date, time, reason for appointment and provider, surgery schedules, etc.

4. Insurance/Financial information – source of payment, account balance, account for billing, etc.

5. Other elements that constitute Protected Health Information as such term is defined by HIPAA.

C. Confidential Information: Both Protected Health Information and Confidential Proprietary Information.

D. Confidential Proprietary Information: Business and operational information of Billings Clinic, including employment-related information.

E. Designated Record Set: A group of records maintained by Billings Clinic that constitute the medical records and billing records about a patient or used, in whole or in part, by or for Billings Clinic to make treatment decisions about the patient.

F. HIPAA: The Administrative Simplification provisions (Subtitle F of Title II) of the Health Insurance Portability and Accountability Act of 1996 and regulations promulgated thereunder by the U.S. Department of Health and Human Services including the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164 of the Code of Federal Regulations, Subparts A & E ("Privacy Rule"), the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Rule"), all as amended and implemented from time to time.

G. Minimum Necessary: The minimum amount of Confidential Information needed to perform an appropriate task related to treatment of the patient, Payment, or healthcare operations of Billings Clinic or the User.

H. Organizational User: A hospital, physician practice, or other health care facility or organization, that has been authorized to have access to the System and that shall be responsible for the actions and omissions of its Workforce.

I. Payment: The activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

J. Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the System.

K. System: Computer software, equipment, systems, techniques, documentation, reports, screens, and other material used, developed, or included by Billings Clinic in its electronic system, including the electronic health record.

L. Treatment: Provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers, relating to a patient for health care from one health care provider to another.

M. User: An Authorized User or an Organizational User.

N. Workforce: Owners, directors, officers, employees, students, volunteers, agents, and other persons whose conduct in the performance of work for the Organizational User is under the direct control of the Organizational User, including physicians and other health care providers who provide services for or through the Organizational User.

## REQUIREMENTS AND PRACTICES FOR THE SYSTEM

### 1. Permitted and Required Uses and Disclosures by User.

**1.1 Limitations on Uses and Disclosures.** Subject to the Privacy and Security Commitment for Access to Computerized Confidential Information and this Agreement, Billings Clinic authorizes User to access, use, and disclose Confidential Information through, maintained on, or related to the System solely as provided in this Section and solely in a manner consistent with the requirements of the federal and state law, including but not limited to HIPAA.

**1.1.1** User may access, use, and disclose Confidential Information entered into, contained on, or transmitted or accessed through the System for Treatment and Payment purposes.

**1.1.2** User may access, use, and disclose only the Minimum Necessary Confidential Information as needed related to the purpose for which User made such access, use, or disclosure and as permitted under this Agreement. .

.

**1.2** Subject to the foregoing, each Authorized User:

**1.2.1** Shall accurately declare the Authorized User's relationship with the patient whose Confidential Information is being requested or accessed (Treatment, Payment, or Health Care Operations).

**1.2.2** Shall only access information in the System for a patient with whom User has a need to access for Treatment, Payment, or Health Care Operations relationship.

**1.2.3** If printing privileges are requested and granted to Authorized User, then Authorized User may print sections of Confidential Information from the System for Treatment, Payment, and/or Health Care Operations purposes (subject to Minimum Necessary requirements) for appropriate purposes. Authorized User will follow all legal requirements and policies of its organization regarding the privacy and security of printed documents. Billings Clinic is not responsible for documents once they are printed documents.

**1.2.4** Shall fully comply with, and, if an Organizational User, shall require its Workforce to comply with the HIPAA Minimum Necessary requirements.

**1.3** User shall not give access to the System or Confidential Information contained in the System to any third party for any purpose.

### 2. Access to the System.

**2.1** Billings Clinic reserves the right, in its sole discretion, and without notice, to suspend, limit, or terminate access to the System by any particular person or entity, on a permanent or temporary basis.

**2.2** An individual health care provider may request to become an Authorized User. An Organizational User may make a request on behalf of appropriate Workforce members to become an Authorized User by submitting requests via online request form. Requests should be directed to the Health Information Management Department at Billings Clinic.

**2.3** Billings Clinic shall designate each Authorized User.

**2.4** An Authorized User shall not access or use the System until the Authorized User successfully completes all mandatory training, signs the Privacy and Security Commitment for Access to Computerized Confidential Information, and agrees to at all times, shall comply with this Terms and Conditions of Use, any protocols, policies, and procedures adopted by Billings Clinic relating to the System, and applicable law. Authorized User shall be responsible for the actions and omissions relating to the System and/or Confidential Information entered into, contained on, or transmitted or accessed through the System by Authorized User. Organizational User shall be responsible for the acts and omissions relating to the System and/or Confidential Information entered into, contained on, or transmitted or accessed through the System by any of its Workforce.

**2.5** Organizational User immediately shall notify Billings Clinic, through Billings Clinic's Health Information Management Department, in the event of: (a) any termination as a Workforce member of any Authorized User; (b) addition of any Workforce member who is designated as an Authorized User; (c) change in any Authorized User's employment or practice status that would affect his or her level of access.

**2.6** Billings Clinic, in its discretion, may terminate Authorized User access and profiles.

**2.7** Billings Clinic reserves the right to change the process by which Authorized Workforce are granted access rights to the System upon notice to User.

## 3. Individuals' Rights and Allocation of Responsibilities.

**3.1 Right to Access and Receive a Copy of Protected Health Information.** User acknowledges that, under federal and/or state law, including but not limited to HIPAA, Billings Clinic is obligated to provide access to individuals concerning certain of their Confidential Information contained in a Designated Record Set. If User receives a request for access from an individual, User will immediately notify Billings Clinic's Health Information Management Department. User is not authorized to release or disclose information in a Designated Record Set.

**3.2 Right to Request an Amendment.**

**3.2.1** User acknowledges that, under federal and/or state law, including but not limited to HIPAA, User may receive requests from individuals for amendments to their Confidential Information. User will immediately forward all such requests to Billings Clinic's Health Information Management Department.

**3.3 Right to Accounting of Disclosures.** User acknowledges that under federal and/or state law, including but not limited to HIPAA, covered entities (as such term is defined by HIPAA) are obligated to provide to individuals accountings of certain disclosures of their Protected Health Information. User will forward all requests for an accounting of disclosures to Billings Clinic's Health Information Management Department.

**3.4 Right to Request Restrictions on Use and Disclosure.** User acknowledges that, under federal and/or state law, including but not limited to HIPAA, covered entities (as such term is defined by HIPAA) are obligated to allow individuals to request restrictions on certain uses and disclosures of the individuals' Confidential Information. User will promptly notify the Billings Clinic Health Information Management Department of any individual requests for restrictions on use of disclosures of Confidential Information. User shall not, under any circumstances, bind any other user or Billings Clinic regarding any such restrictions.

**3.5 Right to Alternative Communications.** User acknowledges that, under federal and/or state law, including but not limited to HIPAA, covered entities (as such term is defined by HIPAA) are obligated to comply with reasonable requests for alternative means of communicating Confidential Information to an individual. User will promptly notify the Billings Clinic Health Information Management Department of any individual requests for alternative means of communicating Confidential Information. User shall not, under any circumstances, bind another user or Billings Clinic with regard to any alternative communication.

**3.6 Response to Subpoenas.** User shall immediately provide notice to the Billings Clinic Health Information Management Department of any subpoenas, discovery requests, search warrants, and court orders, regarding Confidential Information entered into, contained on, or transmitted or accessed through the System. User shall cooperate fully with all Billings Clinic's instructions relating to protecting or disclosing such Confidential Information.

**3.7 Notice of Privacy Practices.** User acknowledges that, under federal and/or state law, including but not limited to HIPAA, User is obligated to develop and provide to certain individuals its notice of privacy practices related to the User's private healthcare practice as a covered entity under HIPAA. User shall comply with applicable law in, and is solely responsible for, developing and providing its notice of privacy practices to such individuals. Such notice shall adequately describe uses and disclosures through the System that User may make in connection with User's activities. Any such notice of privacy practices' provisions that describe the System shall be distributed to individuals or utilized by the User only after prior approval of the System description by the Billings Clinic Privacy Officer.

## 4. User Identification and Password Security

**4.1 User Identification.** Billings Clinic authorizes Authorized User to use the user identification ("User ID") assigned by Billings Clinic. User acquires no ownership rights in the Authorized User ID, and such User ID may be revoked or changed at any time in Billings Clinic's sole discretion. User shall comply with security safeguards for User IDs to prevent disclosure to and use by unauthorized persons. Each Authorized User shall have and use a unique identifier and password. Authorized User shall not use a unique identifier or password attributable to another person. Authorized User shall be responsible for all damages and costs and be bound by any unauthorized use of the User ID, any unique identifier, or any password.

**4.2 Password Access.** All access to the System will be through password security that is under the direction of the Billings Clinic Information Services ("IS") Department.

**4.3 Password Control.** The Authorized User shall set his or her own password in compliance with Billings Clinic policy standards and guidelines.

**4.4 User Accountability.** User is accountable for anything done under his, her, or its password.

**4.5 Confidentiality of Password.** It is the User's responsibility to maintain the confidentiality of his or her password. No User with an assigned password may disclose the password to any other person or attempt to learn another person's password.

**4.6 Changing Passwords.** Passwords will be changed:

**4.6.1** As prompted by Billings Clinic.

**4.6.2** At the request of an Organizational User, when an Authorized User who has or knows a password is terminated or leaves for any reason.

**4.6.3** At the request of any Authorized User, for his or her own password.

**4.7 Workstations.** No terminal, laptop computer or portable electronic device where Confidential Information could be accessed should be maintained in a condition that would permit unauthorized access.

**4.8 Appropriate Control of Passwords.** Passwords should not be written down or posted where they can be seen or easily discovered by others. For instance, passwords should not be posted on terminals or cabinet doors or carried in a case with a laptop.

**4.9 No Use of Another's Password.** Authorized Users are prohibited from accessing Confidential Information by using a password that is not assigned specifically to them.

**4.10 Access only Pursuant to Job Responsibilities.** Authorized Users are prohibited from accessing Confidential Information, unless authorized to do so as a part of their jobs on a "need to know" basis.

**4.11 Reporting Knowledge of Another's Password.** Authorized Users who acquire or come to know a password that they are not authorized to use must immediately notify the Billings Clinic Health Information Management Department. Persons who notify the Health Information Management Department that they know another person's password, but have not used it or passed it to any other person in violation of this Terms and Conditions of Use, will face no adverse consequences.

**4.12 Reporting Improper Activities.** Anyone observing anyone using a password or accessing the System or Confidential Information in a manner he or she believes may violate this Terms and Conditions of Use should report his or her concern to the Billings Clinic Health Information Management Department or the Billings Clinic Privacy Officer.

**4.13 Billings Clinic's Right to Monitor.** Billings Clinic has the right to monitor and audit, without prior notice, both individual usage of the System and the content created, stored, sent, or received on the System. Any Authorized User who uses the System recognizes that he or she does not have right of privacy with respect to use of the System and waives any such right as a condition of receiving a password.

**5. Minimum Necessary Access.** Authorized Users may access Confidential Information only when they have a need to know related to performance of their jobs or treatment of patients.

**6. User Obligations.** User shall comply, and, if User is an Organization User, shall require its Workforce to comply, with the following requirements:

**6.1 Compliance with Law.** User shall comply with federal, state, and local law and will not make any illegal use of the System. User shall not act or fail to act in a manner that would cause Billings Clinic or another user of the System to not be in compliance with any federal, state, or local law. User is responsible for its own compliance efforts including compliance with HIPAA; provided, however, that User will comply with any compliance efforts on the part of Billings Clinic when so requested. Compliance with this Terms and Conditions of Use does not guarantee that User will be in compliance with federal, state, or local law, including HIPAA.

**6.2 Compliance with Billings Clinic's Requirements.**

**6.2.1** User shall comply with the Privacy and Security Commitment for Access to Computerized Confidential Information, this Terms and Conditions of Use, and all Billings Clinic protocols, policies, and procedures of Billings Clinic applicable to the System and Confidential Information.

**6.2.2** Organizational User shall be responsible for and shall require its Workforce to comply with the Privacy and Security Commitment for Access to

Computerized Confidential Information, this Terms and Conditions of Use, and all applicable Billings Clinic protocols, policies, and procedures.

**6.3 Safeguards.** User shall implement and use appropriate administrative, physical, technical, and procedural safeguards to protect the privacy, security, confidentiality, integrity, and availability of Confidential Information entered into, contained on, or transmitted or accessed through the System, to protect against reasonably anticipated threats, and to prevent use or disclosure of such Confidential Information other than as required or permitted by this Terms and Conditions of Use or required by law. Such safeguards shall comply with federal, state, and local requirements including but not limited to HIPAA. Among other things, Organizational User shall maintain an appropriate level of security with regard to all Workforce, systems, and administrative processes used by User to transmit, store, process, or otherwise handle Confidential Information. User shall be responsible for establishing appropriate security management processes, security incident processes, contingency plans, audit processes, facility access controls, workstation use controls and security, device and media controls, authentication procedures, and appropriate security policies and procedures.

**6.4 Workforce.** Organizational User shall require all Organizational User's Workforce who are Authorized Users to sign the Privacy and Security Commitment for Access to Computerized Confidential Information. Organizational User shall discipline Workforce who violate any such requirement, up to and including termination. Organizational User also shall cooperate with Billings Clinic with regard to administering sanctions against User's Workforce for violations identified by Billings Clinic as a result of its investigations, audits, or otherwise.

**6.5 Training.** Organizational User shall train all Workforce on federal and state privacy, security, and confidentiality requirements, including but not limited to HIPAA and its minimum necessary and security awareness requirements, as well as the requirements imposed by the Privacy and Security Commitment for Access to Computerized Confidential Information, this Terms and Conditions of Use, and Billings Clinic protocols, policies, and procedures. Organizational User shall ensure that its training programs comply with the minimum requirements established by Billings Clinic. Further, all Authorized Users shall complete all training sessions as may be required by Billings Clinic from time to time.

**6.6 Privacy Official, Security Official, and Contact Person.** Organizational User shall have designated a privacy official and security official who are responsible, in part, for ensuring compliance with this Terms and Conditions of Use by Organizational User and Authorized Users who are members of its Workforce. Organizational User shall have designated a contact person to receive complaints and answer questions concerning privacy-related issues. The privacy official, security official, and contact person shall provide notifications to Billings Clinic with respect to relevant issues concerning the System and cooperate with Billings Clinic investigation, audit, or similar compliance activity.

**6.7 Abuse of the System.** User will not permit or allow others to: (a) abuse or fraudulently use the System, including but not limited to unauthorized access or attempted unauthorized access, unauthorized alteration, or unauthorized destruction of a user's information or information about any individual maintained on the System; (b) use the System in a manner that causes interference or tampers with another user's use of the System; or (c) uses the System in a manner that violates this Terms and Conditions of Use or Billings Clinic protocols, policies, and procedures.

**6.8 User's Responsibility.** USER WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO THE SYSTEM OR ANY COMPUTER SYSTEM, ANY LOSS OF DATA, ANY DAMAGE OR DESTRUCTION OF DATA, INCLUDING ANY CONFIDENTIAL INFORMATION, OR ANY IMPROPER USE OR DISCLOSURE OF INFORMATION ENTERED INTO, CONTAINED ON, OR TRANSMITTED OR ACCESSED THROUGH THE SYSTEM CAUSED BY USER, USER'S WORKFORCE, OR ANY PERSON USING USER ID, USER'S PASSWORD, OR A UNIQUE IDENTIFIER OR PASSWORD OF ANY AUTHORIZED USER WHO IS A MEMBER OF ORGANIZATIONAL USER'S WORKFORCE.

**6.9 Maintenance of Security.** User is solely responsible for the security of its own computer systems and for its access to and connection with the System. User shall implement security measures with respect to the System consistent with best practices, this Terms and Conditions of Use, and Billings Clinic protocols, policies, and procedures. User shall maintain a system to back-up the contents of its computers and shall be solely responsible for the loss of any data or software regardless of cause. Notwithstanding the above, User shall not create, download or maintain in any form, any copies of System content (including Confidential Information) without the express written consent of Billings Clinic. Without limiting the generality of the foregoing, User shall:

**6.9.1** Ensure the confidentiality, integrity, and availability of all Confidential Information that User creates, receives, maintains, or transmits;

**6.9.2** Protect against any reasonably anticipated threats or hazards to the security or integrity of Confidential Information;

**6.9.3** Protect against any reasonably anticipated uses and disclosures of such information that are not permitted under federal or state law or this Terms and Conditions of Use;

**6.9.4** With respect to Organizational Users, ensure compliance with this Terms and Conditions of Use and federal and state law by its Workforce;

**6.9.5** Prevent, detect, contain, and correct security violations;

**6.9.6** With respect to Organizational Users, ensure that all members of the Workforce have appropriate access to Confidential Information through the System and prevent Workforce who are not Authorized Users from obtaining access to the System;

**6.9.7** Implement policies and procedures for authorizing access to the System that are consistent with federal and state law, including but not limited to HIPAA;

**6.9.8** Limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed;

**6.9.9** With respect to Organizational Users, implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific work station or class of work station that can access Confidential Information through the System;

**6.9.10** Implement physical safeguards for all work stations and portable devices that access the System;

**6.9.11** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Confidential Information into and out of a facility, and the movement of those items within the facility;

**6.9.12** With respect to Organizational Users, implement technical policies and procedures for electronic information systems, including the System, that maintain Confidential Information to allow access only to those persons or software programs that have been granted access rights;

**6.9.13** Implement hardware, software, and/or procedural mechanisms that record and examine activity in the System and other information systems that contain or use Confidential Information;

**6.9.14** Protect Confidential Information from improper alteration or destruction;

**6.9.15** Verify that a person or entity seeking access to the System or to Confidential Information contained on the System is the one claimed;

**6.9.16** Implement technical security measures to guard against unauthorized access to the System and to Confidential Information that is being transmitted over an electronic communications network; and

**6.9.17** Monitor and identify security incidents and unauthorized access or disclosure of Confidential Information and immediately report significant security incidents and any unauthorized access or disclosures to Billings Clinic.

**6.10 Viruses.** User shall ensure that no programs or devices, such as viruses, worms, Trojan horses, or other forms of malicious or potentially destructive computer code or computer sabotage, will be placed within the System that could disrupt use of the System, or any system, equipment, or software to which the System is interfaced or connected or could destroy, alter, or damage data or make data

inaccessible or delayed, or could permit any unauthorized personnel to access the System.

**6.11 Notification.**

**6.11.1** User immediately shall notify the Billings Clinic Privacy Officer in the event User discovers or suspects: (a) any unauthorized use of or access to the System; (b) any use or disclosure of Confidential Information contained on the System not permitted by this Terms and Conditions of Use; (c) any action or omission that may adversely affect the confidentiality, privacy, security, availability, or integrity of any Confidential Information; (d) the recognition or introduction of any virus or any malicious or destructive programs; or (e) any actual or suspected breach of this Terms and Conditions of Use or Billings Clinic protocols, policies, or procedures that affects or may affect Confidential Information entered into contained in, or transmitted or access through the System.

**6.11.2** User shall immediately report to the Billings Clinic Privacy Officer any Security Incident of which it becomes aware.

**6.12 Remedy of Security Incident.** User shall cooperate fully with Billings Clinic with respect to any investigation, audit, or other compliance activity related a Security Incident and shall take all reasonable actions, consistent with Billings Clinic recommendations or instructions, to cure the Security Incident if such incident resulted in a breach of data, and prevent future Security Incidents, and to mitigate the effects of the Security Incident or breach. If in Billings Clinic's opinion, a Security Incident has affected or may affect any other System user or any individual whose Confidential Information is contained on the System, then Billings Clinic, in its discretion, may notify such user or individual of the Security Incident or may require User to immediately notify such user or individual of the Security Incident.

_____ _____

Signature Date

_____

Printed Name (and Title for signatories for Organizational Users)