

PRIVACY POLICIES AND PROCEDURES

POLICY—Adoption. We will adopt and implement written privacy policies and procedures for protected health information designed to comply with our obligations under the Privacy Rules. These Privacy Policies and Procedures satisfy this obligation.

PROCEDURE—Implementation and Compliance. Each member of our workforce with access to protected health information must, at all times, comply with the policies and follow the procedures set out in these Privacy Policies and Procedures. Consult with the manager of your department or our Privacy Officer before you use or disclose protected health information, if there is any doubt regarding whether such use or disclosure is permitted by these Privacy Policies and Procedures or by the Privacy Rules.

POLICY—Revisions. Only our appropriate senior management, with the advice and concurrence of our Privacy Officer may change these Privacy Policies and Procedures.

Mandatory Revision. We will promptly change these Privacy Policies and Procedures as necessary and appropriate to comply with each material change in the Privacy Rules or other applicable federal or state privacy law, and promptly implement the change.

We will promptly make appropriate revisions to our Privacy Practices Notice whenever the change in law materially affects the accuracy of the Notice content.

Elective Revision. We may change our privacy practices at any time by amending these Privacy Policies and Procedures, provided they remain in compliance with the Privacy Rules and all other applicable federal and state privacy law.

If the change materially affects the content of our Privacy Practices Notice, we will make corresponding changes to our Notice. We will not implement the change in these Privacy Policies and Procedures until after the effective date of the revised Notice.

POLICY—Documentation. We must retain, on paper or electronically, each set of our Privacy Policies and Procedures, and all documentation reflecting each change in our Privacy Policies and Procedures and any corresponding change in our Privacy Practices Notices, until 6 years after the later of their creation or last effective date.

PROCEDURE—Documentation. You must furnish our Privacy Officer any documentation regarding changes in our Privacy Policies and Procedures and corresponding changes in our Privacy Practices Notices. Our Privacy Officer will retain each set of our Privacy Policies and Procedures and all documentation reflecting changes in them and in our Privacy Practices Notices until 6 years after the later of their creation or last effective date.

PRIVACY PERSONNEL, TRAINING, WORKFORCE MANAGEMENT,
ADMINISTRATIVE PRACTICES

POLICY—Privacy Personnel.

Privacy Officer. Our Privacy Officer is responsible for developing, maintaining, and implementing these Privacy Policies and Procedures, and for overseeing our full compliance with these Privacy Policies and Procedures, the Privacy Rules, and other applicable federal and state privacy law.

Our Privacy Officer is _____

Telephone: ___ Fax: _____

E-mail: _____

Office: _____

PROCEDURE—Delegation. Our Privacy Officer may delegate specific duties and responsibilities to designees with the documented concurrence of appropriate senior management.

PROCEDURE—Contact Office Supervision. Our Privacy Officer will supervise, direct, and control the operations of, and the personnel assigned to, our contact offices.

POLICY—Workforce Training. Each member of our workforce who may have access to or use of protected health information will receive training on our Privacy Policies and Procedures, as necessary and appropriate for the member to carry out his or her job functions.

PROCEDURE—Training Timing.

Current Workforce. Existing workforce must complete privacy training by April 14, 2003 (our Privacy Rules compliance date).

New Hires. Newly hired members of our workforce must receive privacy training before they may have access to or use of protected health information.

Retraining. Existing workforce members must receive retraining no later than 45 days after there is material change in their job functions or in our Privacy Policies and Procedures that affects their access to or use of protected health information.

PROCEDURE—Training Documentation. Our Privacy Officer will document completion of training of each workforce member on our Privacy Policies and Procedures..

POLICY—Workforce Sanctions. Workforce members who violate our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law will be subject to disciplinary action, including employment termination, consistent with the sanctions developed,

documented, and disseminated by our Privacy Officer in coordination with our Human Resources Manager.

PROCEDURE—Workforce Sanctions. Our Privacy Officer will coordinate with our Human Resources Director to develop, document, and disseminate to the Directors of each department a list of sanctions for workforce members who violate our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law. The Directors will disseminate this list of sanctions to each workforce member in their departments.

PROCEDURE—Reporting Workforce Privacy Violations. Each member of our workforce is obligated to report promptly any suspected violation of our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law to the department manager or our Privacy Officer. Reports may be made anonymously. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Privacy Officer.

POLICY—Mitigation. We will have and implement contingency plans to mitigate any deleterious effect of an improper use or disclosure of protected health information by a member of our workforce or by our business associates.

PROCEDURE—Mitigation Implementation. Our Privacy Officer will coordinate with our Human Resources Manager to develop contingency plans to mitigate, to the extent possible, any deleterious effect of improper use or disclosure of protected health information by a member of our workforce or by our business associates in violation of these Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law. Each member of our workforce will cooperate fully with the mitigation efforts of our Privacy Officer.

POLICY—Retaliatory Acts. We will not, and we will not tolerate any workforce member who attempts to, intimidate, threaten, coerce, discriminate or retaliate against an individual who:

Exercises any right, including filing complaints, under the Privacy Rules or other privacy laws.

Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by HHS or other appropriate authority.

Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rules (provided the opposition is reasonable and does not involve illegal disclosure of protected health information).

PROCEDURE—Prevention of Retaliatory Acts. A member of our workforce who suspects that another workforce member has violated the ban on retaliatory acts must report the suspicion to our Privacy Officer or our Legal Department. Reports may be made anonymously. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Privacy Officer.

POLICY—Waivers. We will not require an individual to waive any right under the Privacy Rules, including the right to complain to HHS, as a condition of providing claims payment, enrollment or benefits eligibility to the individual.

PROCEDURE—Prevention of Waivers. A member of our workforce who suspects that another workforce member has violated this ban on waivers must report the suspicion to our Privacy Officer. Reports may be made anonymously. Each member of our workforce must cooperate fully with any investigation, corrective action or sanction instituted by our Privacy Officer.

POLICY—Documentation and Record Retention. We will retain the documentation required by our Privacy Policies and Procedures and the Privacy Rules until 6 years after the later of its creation or last effective date.

DATA SAFEGUARDS

POLICY—Data Privacy Protection. We will implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to secure the privacy of protected health information against any intentional or unintentional use or disclosure in violation of these Privacy Policies and Procedures or the Privacy Rules. These safeguards shall include affirmative action to delete outdated and incorrect facsimile transmission or other telephone transmittal numbers from computer, facsimile, or other data bases. When health care information is transmitted electronically to a recipient who is not regularly transmitted health care information from the health care provider, the health care provider shall verify that the number is accurate prior to transmission

PROCEDURE—Data Privacy Protection. Our Privacy Officer, in conjunction with our Chief Information Officer, will augment these Privacy Policies and Procedures with such additional data security policies and procedures as appropriate for our organization to have reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the protected health information we maintain against any reasonably anticipated unauthorized use or disclosure, intentional or unintentional, or any reasonably anticipated threat or hazard to the privacy, security or integrity of the protected health information. These additional data security policies and procedures will ensure compliance by our officers and other workforce members with these Privacy Policies and Procedures, the Privacy Rules, and such other policies and procedures as may be adopted to implement our compliance obligations under the Privacy Rules.

PROCEDURE—Departments. The Directors of each department will implement our policies and procedures regarding the privacy, security, and integrity of protected health information. Any question regarding the meaning or application of any provision of these Privacy Policies and Procedures or any other policy and procedure we may adopt must be addressed to our Privacy Officer before you act.

COMPLAINTS AND HHS ENFORCEMENT

POLICY—Complaints. We will timely investigate and appropriately respond to each written complaint received by our contact offices or a workforce member regarding our compliance with these Privacy Policies and Procedures or the Privacy Rules.

PROCEDURE—Complaint Response. Only our Privacy Officer may respond to a complaint on our organization's behalf. Our Privacy Officer will process a complaint as follows:

Investigate the complaint and document the investigation, findings, and conclusions.

Notify the complainant of our resolution of the complaint.

Institute appropriate action to correct the matters complained of, if corrective action is warranted.

Mark any portion of the complaint form that is subject to the attorney-client or attorney work product privilege as "privileged and confidential," furnish a copy of that form to the Privacy Officer and retain the original for the Privacy Officer file.

PROCEDURE—Departments. The Director of each department must ensure the full and timely cooperation of department workforce members with complaint investigation conducted by our Privacy Officer regarding compliance with our Privacy Policies and Procedures or the Privacy Rules.

POLICY—HHS Enforcement and Compliance Cooperation. We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of our organization. Our Privacy Officer will keep sufficient non-privileged records of our compliance to be able to submit compliance reports in the time, manner, and with the information HHS requests to ascertain our compliance.

PROCEDURE—Compliance Cooperation. Our legal counsel, in conjunction with our Privacy Officer, will coordinate our response to any HHS compliance review, complaint investigation or other inquiry, to ensure that all applicable obligations of our organization are fulfilled and all applicable rights and privileges of our organization are preserved and protected.

He/she will also, in conjunction with our Privacy Officer, will arrange for HHS to have access to our facilities, books, records, accounts, and other non-privileged information sources (including protected health information without individual authorization or notice).

Our legal counsel, in conjunction with our Privacy Officer, will endeavor to obtain non-privileged information required by HHS that is in the exclusive possession of our business associates, other agents, institutions or persons who fail or refuse to furnish the information directly to HHS.

PROCEDURE—Departments. You must immediately notify our Privacy Officer of any inquiry from HHS or any other government Officer. You must await instruction from our legal

counsel or our Privacy Officer before responding to these inquiries or providing any documents or other information on behalf of our organization.

Do not obstruct or interfere with any lawful process, warrant, order or subpoena that may be presented. If the officers insist they have the right of immediate search and seizure of our organization's records, equipment or other matters specified in the process presented, do not obstruct or interfere with them. Instead, use your best efforts to contact Administration and to observe and document everything that the officers search, seize, say, and do.

PROCEDURE—Verification. You must verify the identity and authority of an HHS representative seeking protected health information before you may disclose the protected health information to the HHS representative.

PROCEDURE—Minimum Necessary. You are not required to limit to the minimum necessary the protected health information disclosed to HHS for complaint investigation or compliance enforcement or review.

PROCEDURE—Disclosure Log. You must log each disclosure to HHS for accounting.