PROXY ACCESS DISCLAIMER

You, the patient, are now accessing online medical information for another person. By clicking the Accept button, you are verifying that you have the right to access this information, granted to you by the clinic. If you feel that you've received this access in error, please contact the clinic.

We think it is important for you to know how we handle information we communicate via the Internet. This statement outlines our practices and our sensitivity to your right to privacy. We reserve the right to revoke access at any time for any reason.

Response to Electronic Communication - Your clinic will make its best effort to provide a timely response to electronic inquiries. In some cases, the clinic staff that needs to respond to an electronic inquiry or other communication may not be immediately available so a proxy of a MyChart patient should allow at least three (3) business days for a response. Accordingly, emergency situations requiring immediate attention should not be submitted electronically.

Furthermore, with respect to any electronic communications which you send, we are only able to respond to such communications based on the information you provide. If there is insufficient information provided, we will be unable to provide accurate and reliable services.

Website Links - MyChart may offer links to related medical websites not managed by your clinic. These website link(s) are for patient or proxy informational purposes only. We do not endorse and have not verified the accuracy of the information in/on these websites, and you should not rely on any of the information found on the websites for purposes of treatment or diagnosis.

Email Privacy - Notification messages regarding information in MyChart may be sent to your email address. Any person with access to this email account will be able to see this notification. This could include the patient's spouse, employer or anyone else that can access the account. Although no private medical information will be sent, the notification that new medical information is available by accessing MyChart may be information that a patient or a proxy would not want others to know. Please take this into account when providing an email address.

Please know that if you send us an email communication, it may be shared with the clinic staff that assists the physician in providing the patient's medical care. A patient's confidential medical information on MyChart will be accessible only to appropriate clinical staff.

Security and Confidentiality - We afford the same degree of confidentiality to medical information stored on MyChart as is given to medical information stored by your clinic in any other medium. Your clinic is committed to protecting the confidentiality of this medical information. We limit your clinic employees' access and ability to enter or view information based upon their role in your care. Firewalls, passwords, encryption and audit trails are further used to safeguard your information. We shall identify the records released and note the time and date of access each time a patient accesses MyChart. We have taken steps to make all information received from our online visitors as secure as possible against unauthorized access and use.

For other than general information viewing, MyChart must be accessed with a Secure Sockets Layer (SSL) compatible browser or terminal (Netscape or Internet Explorer versions 3.0 or greater). Our SSL

Web server uses authentication and offers the highest level of encryption technology commercially available (128-bit RC4).

You can tell when you are secure by looking at the location (URL) field. If the URL begins with https:// (instead of http://), the document comes from a secure server. This means your data cannot be read or deciphered by unauthorized individuals. You can tell whether you are truly connected to your clinic by viewing the digital certificate. This certificate verifies the connection between the clinic server's public key and the server's identification.

User names and passwords provide two layers of authentication and are stored in an encrypted database that is isolated from the Internet.