Institutional Handbook of Operating Procedures Policy 02.19.08	
Section: General Administrative Policies and Service	Responsible Vice President: Senior Vice President & General Counsel
Subject: Computers/Automated Information Systems	Responsible Entity: Office of Information Security

I. Title

Secure Chat Messaging

II. Policy

Secure Chat Messaging is a secure way to communicate brief, non-emergent information between individuals or members of a patient care team. Messages can be exchanged using Hyperspace, Haiku, and Canto. They are not part of the legal medical record and may be subject to eDiscovery requests, Texas Public Information Act requests, or other types of legal inquiries. Secure chat is not a substitute for clinical decision making or official documentation and cannot be used to submit orders in the electronic health record. This platform shall **not** be used to communicate critical or time sensitive clinical information.

1. Secure Chat is an alternative communication platform; its use is optional.
2. Secure Chat is the only authorized messaging platform at UTMB. The use of non-secure SMS, IMessage, or similar types of technology for patient care communication is prohibited.-
3. Prior to enrollment in Secure Chat, all users must attend required training offered through the UTMB ITS training department.
4. Personal messaging is not permitted via Secure Chat. Work related communications are permitted.
5. All patient care messages shall be professional and in compliance with UTMB's Standards of Conduct Guide**.**
6. Secure Chat shall not be used to communicate urgent or critical care results.
7. Secure Chat shall not be used to send initial physician consults. A consult order must be placed in Epic. Follow-up messages regarding consults are allowed.
8. Messaging orders are not permitted.
9. Messages shall be simple, short, and to the point. Use only the minimum information needed to communicate with recipients. Abbreviations and acronyms should only be used when the sender is confident that recipient(s) are familiar with their meaning.
10. All active Epic users are available on Secure Chat. Users shall pay attention to recipient lists when chatting about a patient in a group. Only those who are actively involved in the patient's care should be listed.
11. Patient treatment information sent via Secure Chat must have the relevant information documented separately in the patient's medical record.
12. Unless a read receipt has been received, senders should not assume messages have been read by the recipient.
13. Much like an email, messages with inaccurate or incomplete information or information sent to the incorrect user cannot be retracted or deleted. The sender must contact the recipient(s), notify them of the error, and resend the message with the accurate information to the correct individuals.

14. Messages requiring a timely response from the recipient(s) that have not been responded to within 10 minutes, shall be confirmed using an alternative communication method, i.e., telephone, pager, etc.
15. Taking photographs, screen shots, or any replication of texts sent via Epic Secure Chat Messaging is prohibited
16. Secure Chat Messages are subject to all legal discovery requests.
17. Messages with PHI information will be retained for a period of 90 days. Non-PHI related messages will be retained for 30 days. Once retention thresholds have been met, all messages will be purged from the system.

III. Relevant Federal and State Statutes

Code of Federal Regulations Title 45 part 164, Subparts A, B and C, HIPAA Privacy and Security
Texas Administrative Code Title 1 Part 10 Chapter 202 Subchapter C, Information Security Standards

IV. Relevant System Policies and Procedures

UTS 165 Information Resource Use and Security Policy

V. Related UTMB Policies and Procedures

IHOP - 02.19.06 - Information Resource Security
IHOP - 02.01.03 - Release of Information under the Texas Public Information Act
IHOP - 06.02.00 – Maintaining Patient Confidentiality through the Appropriate Use and Disclosure of PHI
IHOP - 06.02.29 - De-Identification of PHI

VI. Additional References

Standards of Conduct Guide: Working with Integrity

VII. Dates Approved or Amended

Originated:11/09/2022	
Reviewed with Changes	*Reviewed without Changes*

VIII. Contact Information

Office of Information Security
(409) 772-3838