Remote Monitor Request Form

To provide access to remote monitoring at Stephenson Cancer Center all monitors must agree to download the following systems and work with internal IT department for any connection issues.

Before signing below, please confirm with your IT department if this is acceptable.

Send completed form to Data Specialist to schedule a remote visit.

☐ **VMware Horizon Client:** To remotely view EMR system by creating a network account

☐ **Duo Two-Factor Authentication Account:** An App downloaded on mobile phone or tablet to provide a second form of identification to allow access to network account

Print name

Signiture

Date

Remote Monitor Request Form

Personal Information

Name

Email Address

Organization

Protocol Number

Will your visit **REQUIRE** a Co-Monitor? ☐ No ☐ **Yes** ***Co-Monitor requests require special permission***

Co-Monitor Name

Reason for request

☐ Check this box if you are requesting to reschedule a previously scheduled visit.

Requests

Which system access and documents do you need while on campus?

☐ Velos (regulatory system)
☐ Electronic Medical Record
☐ Pharmacy Documents

Visit Details

Preferred remote visit dates (please list 2 potential date options)

First Choice

Second Choice

Which staff members do you need to speak via teleconference with during your remote visit?

☐ Data Specialist
☐ Principal Investigator or Sub-Investigator
☐ Other

Are there any additional details that we need to know about your visit?

Please e-mail this completed form to the Data Specialist for your study.

INFORMATION TECHNOLOGY

Computer Account Request

If user will need to take HIPAA and Sexual Harassment training, please have your payroll coordinator submit an ePAF in PeopleSoft HC as a volunteer which will create the account automatically versus sending in this request.

**** Please Print CLEARLY ****

New User's Name:_____
LAST FIRST MIDDLE INITIAL

Last 4 digits of SSN:_____ (Required)

OUHSC Department:_____ Phone #_____

New User's Department Supervisor:_____ Phone # _____

Name of Affiliated Organization: _____

Length of contract with OUHSC: _____

After completing above, Ecopy/fax both pages of this form to your DEPARTMENT COMPUTER SUPPORT PERSONNEL for below authorization.

Computer Account Sponsor Only

(Sponsor is authorized in writing and is usually someone in the department's computer support area)

As a computer account sponsor, I (1) agree to assume limited responsibility for the use of this user account as outlined in the ***Account Sponsor Responsibilities,*** (2) state that this user account is necessary to conduct university business or for an official university activity/endeavor, and (3) inform the Service Desk when the account is no longer needed.

Sponsor's Name:_____ Title:_____
Print or Type

Sponsor's Signature:_____ Date:_____

Account Sponsor ~~ utilize one of the following to submit the forms: Ecopy to ServiceDesk@ouhsc.edu; fax to 271-2126; send hardcopy to Account Management, ROB 501

INFORMATION TECHNOLOGY

Acceptable Use of Information Systems

General Principles

Access to computer systems and networks owned, operated, or provided by the University is predicated on compliance with certain responsibilities and obligations and is granted subject to University policies and local, state and federal laws. By using University information systems or computing resources, you agree to abide by and comply with the applicable policies, procedures and laws. Acceptable use must be ethical, reflect academic honesty, and show responsible use in the consumption of shared resources. Acceptable use also demonstrates respect for intellectual property, ownership of data, system security mechanisms, and freedom from intimidation and harassment. Information created or stored on University computer resources, networks and systems may be subject to the Oklahoma Open Records Act.

In making acceptable use of information resources you **MUST**:

- Comply with all University policies, procedures, and local, state, and federal laws
- Use resources only for authorized administrative, academic, research or clinical purposes; or other University business
- Protect your user-ID and system from unauthorized use. (you are responsible for all activities on your user-ID or that originate from your system);
- Access only information that is your own, that is publicly available, or to which you have been given authorized access;
- Comply with all copyright laws, licensing terms, patent laws, trademarks, trade secrets and all contractual terms
- Be responsible in your use of shared resources (refrain from monopolizing systems, overloading networks, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.)

In making acceptable use of information resources you **MUST NOT**:

- Use another person's system, files, or data without express authorization
- Use another individual's user id or password
- Use computer programs to decode passwords or access control information;
- Attempt to circumvent or subvert system or network security;
- Engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to or sharing of university data;
- Use university systems for commercial, private, personal, or political purposes, such as using electronic mail to circulate advertising for products or for political candidates;
- Harass or intimidate another person including, but not limited to, broadcasting unapproved, unsolicited messages, repeatedly sending unwanted or threatening mail, or using someone else's name or user-id
- Waste computing resources or network resources including, but not limited to, intentionally placing a program in an endless loop, printing excessive amounts of paper, or sending chain letters or unapproved, unsolicited mass mailings
- Attempt to gain access to information or services to which he/she has no legitimate access rights
- Engage in any other activity that does not comply with the general principles presented above, university policies and procedures, or applicable law;

Enforcement

The University considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy, monitor and/or examine any files or information residing on University systems, networks, or computing resources allegedly related to unacceptable use, and to protect its systems and networks from events or behaviors that threaten or degrade operations. Violators are subject to disciplinary action including, but not limited to, penalties outlined in the Student Code, Staff Handbook, or Faculty Handbook. Offenders also may be prosecuted under laws including, but not limited to, the Communications Act of 1934 (amended), Family Educational Rights and Privacy Act of 1974, Computer Fraud and Abuse Act of 1986, Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, Digital Millennium Copyright Act, Health Insurance Portability and Accountability Act, Electronic Communications Privacy Act, Oklahoma Open Records Act, and state conflicts of interest laws.

Individuals using computer systems owned by the University do so subject to applicable laws and University policies. The user assumes all risk of loss of materials or data or damage thereto. The University disclaims any responsibility and/or warranties for information and materials residing on non-University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of the University, its faculty, staff or students. These guidelines should not be construed as a limit on any individual's right under the Constitution of the United States or the laws of Oklahoma.

--- Policy Approved by the Senior Vice President and Provost, January 19, 2000, Revised August 21, 2003

Instructions: Please ***print*** your name and your primary department or college in the box below, sign and date this policy agreement (page 1).

I have read and understand the above policy and agree to abide by this policy in my use of OUHSC computer resources.

Computer User (print): _____, _____ _____ _____

Last Name | First Name | Middle Initial | Department or College

User's Signature: _____ Date: _____

Hand-written signature

Electronic Medical Record Access Agreement For External Users
(Signed by the Individual Receiving User ID)

Security, confidentiality, and data integrity are matters of concern for all persons who have access to any University medical record, including Electronic Medical Records, research participant records, and billing records. Each person who accesses these records must recognize these responsibilities and be entrusted in their preservation. This document deals with use of and access to electronic medical records and, as applicable, to paper records as well. You have requested access to and/or are being afforded access to certain medical or billing records as part of Treatment, Payment, or Health Care Operations, as defined by HIPAA.

The following specific principles concerning security, confidentiality, and integrity of the University EMR and its records are applicable to all persons who access the University's medical records.

As a condition of being granted access to the University's medical records, you agree that you will:

- Access only those records that are necessary for the purpose for which your access has been granted as described below. Notify the University Privacy Official (405-271-2033) if you access any records not needed for this purpose.
- Not release your assigned EMR user identification or password (electronic signature/authentication device where applicable) to anyone else, or intentionally/unintentionally allow anyone else to access or alter information using your user identification.
- "Lock" the computer when you leave the workspace by selecting the "CTRL," "ALT," "DEL" keys. You will exit to the logon window when you are not at the workstation.
- Not utilize anyone else's user identification or password to access EMR or alter information.
- Understand that the information accessed through EMR contains sensitive and confidential patient information that may be disclosed only to those authorized under applicable law to receive it.
- Respect the privacy and rules governing the use of confidential information accessible through EMR including, but not limited to, HIPAA and HITECH, and utilize only that information necessary to perform my legitimate duties.
- Understand that all access, attempts to access, and accomplishments of specific functions (e.g., entry and authentication of information, access to records identified or recognized as sensitive, accumulation of unsigned documents) will be monitored and are subject to review by the University at its discretion.
- Respect and maintain the confidentiality of the records and any patient information contained in or printed from EMR and handle, store, use, and dispose of the records and information appropriately and in accordance with applicable law.
- Understand that the authentication (electronically signing) of documents within EMR will be treated as a written signature with all the ethical, business, and legal implications associated therewith.
- Not divulge, copy, benefit personally, alter or destroy, store on unencrypted electronic devices or in unencrypted storage or remove from the premises the records or any information contained within the records in any medium, except as properly authorized by the University and within the scope of your professional duties.
- Not store any University records on any personally-owned or unencrypted electronic devices in the permitted performance of the functions or activities above or transmit them via unencrypted transmission.
- Comply with the OUHSC Acceptable Use of Information Systems Policy. (If you are not given a copy, you agree to request one.)

You understand that you have no right or ownership interest in information within the EMR and that your access or access code may be revoked at any time.

Violators of this Agreement may be subject to loss of EMR access and other action. By signing below, you agree that you have read, understand, and will comply with this Agreement.

Print Name: _____

Signature: _____ Date: _____

Company: _____

Job Title: _____

Purpose for Requested Access: _____

For Administrator Only:
User ID: _____ Activation Date: _____ Deactivation Date: _____

Role(s): _____

Stephenson CANCER CENTER
the UNIVERSITY of OKLAHOMA

CONFIDENTIALITY ACKNOWLEDGEMENT & AGREEMENT FORM

During the course of your activity at Stephenson Cancer Center and its affiliates, you may have access to information which is confidential and may not be disclosed except as permitted or required by law and in accord with Stephenson Cancer Center policies and procedures. In order for Stephenson Cancer Center to properly care for patients and engage in successful business planning, certain information must remain confidential. Improper disclosure of confidential information may cause irreparable damage to Stephenson Cancer Center and the Health Sciences Center. Confidential information includes, but is not limited to:

1. Medical and certain other personal information about patients.

2. Medical and certain other personal information about employees.

3. Medical staff records and committee proceedings.

4. Reports, policies and procedures, marketing or financial information, and other information related to the business of services of Stephenson Cancer Center and its affiliates which has not previously been related to the public at large by a duly authorized representative of Stephenson Cancer Center and the Health Sciences Center.

By signing this Confidentiality Acknowledgment, I acknowledge and agree that:

1. I will only access business information for which I have a legitimate business purpose and approved by a duly authorized representative of Stephenson Cancer Center and the Health Sciences Center.

2. I am obligated to hold confidential information in the strictest confidence and not to disclose the information to any person or in any manner which is inconsistent with this agreement.

3. I will print information only when necessary for a legitimate purpose and approved by a duly authorized representative of Stephenson Cancer Center and the Health Sciences Center. I am accountable for this information until it is destroyed.

I HAVE READ AND UNDERSTAND THIS CONFIDENTIALITY AGREEMENT.

_____ _____

Visitor Signature DATE

_____

Print Name

Stephenson
CANCER CENTER
the UNIVERSITY of OKLAHOMA

CLINICAL TRIAL MONITOR GUIDELINES

The purpose of these Guidelines is to give you an overview of how our site operates in hopes of making your monitoring visit as productive as possible. Please recognize that the Stephenson Cancer Center (SCC) is participating in many research trials. Our goal is to not only protect the confidentiality of the company you work for, but to also protect the confidentiality of our participants and all of the companies we work with. In order to achieve that goal, we require that you comply with these Guidelines so that everyone involved receives the same level of attention and courtesy.

---

1. Please provide a visit confirmation letter at least two weeks prior to visit including:
   - List of personnel who need to be available (i.e., PI, pharmacy staff)
   - Prioritized list of up to 10 patients to be reviewed in sites' Electronic Medical Records (EMR.) Requests for 'all patients' will not be accepted.
   - Prioritized list of documents requested from pharmacy (i.e., Drug Accountability log, temperature logs, shipping receipts, orders, verification of shelf count, lot numbers, etc.)

   Note: The Data Manager will schedule all appointments and will notify the monitor of any unavailable charts or personnel as soon as possible.
2. Only 1 monitor per visit is allowed, unless otherwise approved in advance by appropriate SCC personnel. No more than 3 monitors will be allowed at any time.
3. Monitors must adhere to the University parking policy and may not park in the Stephenson Cancer Center garage or utilize the valet. *(See website for details.)*
4. Upon arrival each day, monitors must check in at the first floor Welcome Desk. Monitors will be issued a badge and key and will proceed to the 5th floor monitoring room.
5. Monitoring Hours: Firmly 8:30-4:30. For security purposes, these hours are strictly enforced. All study materials and monitoring laptops must be locked in the overhead cabinet by 4:30 daily.
6. Monitors must be respectful of others and refrain from discussing patients or study issues in the monitoring room and the surrounding hallways and elevators. Phone conversations are prohibited in these areas, and all cell phones must be kept on silent. All calls must be held in the lobby.
7. Food is prohibited in the monitoring room, except for small snacks and drinks with lids.
8. Monitors may not go to research staff offices, patient care areas, labs, or staff work areas unless escorted by the Data Manager or designee.
9. Monitors must ensure the monitor station is clean and all trash has been thrown away.
10. Monitors shall provide site with a visit follow-up letter within 2 weeks of the visit outlining what was accomplished and any outstanding issues.
11. Subsequent visits will not be scheduled less than 4 weeks from the previous visit.
12. Monitors are not allowed to write in or dismantle a medical chart or reorganize the regulatory binder. Post-it notes may not be placed in subject charts. Making copies of source documents with Patient Health Information (PHI) is prohibited.

Stephenson
CANCER CENTER
the UNIVERSITY of OKLAHOMA

13. Our primary purpose is patient care. Monitors are advised that medical charts they are reviewing will be returned to the clinic IMMEDIATELY if the clinic staff requests it for any reason.
14. Monitors are not allowed to contact clinic, lab, or pharmacy staff directly without prior approval and direction from Data Manager.
15. Prior to having access to PHI or areas that contain PHI, each monitor must sign and return to assigned research staff the University's Confidentiality Agreement, attached to these Guidelines.

We value our relationship, and look forward to working with you. Thank you for your attention to and adherence with these Guidelines, which will help ensure a successful and productive visit.

Best Regards,

Ingrid L. Block, APRN, MS, CNS
Clinical Trials Office Director
Stephenson Cancer Center
University of Oklahoma

Kathleen Moore, MD
Jim and Christy Everest Endowed Chair in Cancer Research
Director, Oklahoma TSET Phase I Program
Stephenson Cancer Center
Associate Professor, Section of Gynecologic Oncology
Director Gynecologic Oncology Fellowship
Department of Obstetrics and Gynecology
University of Oklahoma Health Sciences Center

By signing this document, you agree to adhere to these Clinical Trial Monitor Guidelines.

_____ _____/_____/_____

Monitor Name **Date**