Ticket#_____

IT Remote Access Request

Clear Form

Children's of Alabama

Complete this form and return it to the Customer Support Desk Email: CustomerSupportDesk@childrensal.org | Fax: 205-638-6119

• Applicant Identification

Name: _____ _____ _____
(*Last*) (*First*) (*MI*)

PIN (4 Digits): _____ Department or Company _____

Job Title & Occupation: _____

Please indicate the applicant status: ☐ Employee ☐ COA ☐ UAB ☐ Physician / Clinician

☐ Vendor or Business Associate: _____ ☐ Other: _____

List the names of the applications to be accessed **remotely**: _____

_____

COA User Name: _____ UAB Username: _____ Physician ID: _____

REASON FOR ACCESS: _____

_____ | Device info. _____
Company ID or Name of PC, Tablet, Laptop

E-mail Address: _____ **Cell:** _____

Applicant Signature: _____ **Date:** _____
Physical signature is required

By signing above, I Acknowledge Children's of Alabama Confidentiality, Nondisclosure Agreement, Remote User Policy and Appropriate Electronic Usage Rules of Behavior.

• Children's of Alabama Director must complete this section before submitting the request

Director Signature not required for Medical Providers

Name: _____ **Dept.:** _____

Email: _____ **Phone:** _____

Duration of Use: ☐ **From:** _____ **to** _____ ☐ **COA Employee**

Director's Signature / Date: _____
Physical signature is required

_____ _____
MIS Approval **Date** **Security Approval** **Date** ☐ Citrix ☐ VPN

CHILDREN'S OF ALABAMA
Confidentiality and Nondisclosure Agreement

I understand my legal and ethical duty to maintain and promote the confidentiality and privacy of Children's of Alabama (Children's) confidential patient, employee, and business information. By signing below I (and my employees, subcontractor sand agents if applicable) agree to the following:

1. I am responsible for protecting confidential information used or obtained in the course of my services and for conducting myself in accordance with the applicable laws (i.e. the Health Insurance Portability and Accountability Act-HIPAA and HITECH, Health Information Technology for Economic and Clinical Health Act and the HIPAA Omnibus Rule), standards of the applicable accreditation authorities, and the policies of Children's governing confidential information that apply equally to verbal, written, or electronic information.
2. I will not misuse or be careless with confidential information. I will appropriately shred confidential information and not discard in the trash. I will only access, use, and disclose confidential information as authorized to perform my legitimate duties, on a "need to know" basis for my job/role, and never for my own advantage or for purposes other than its intended use.
3. I will not divulge, copy, release, review, alter, or destroy any confidential information except as properly authorized by Children's. I will never sell any confidential information. I will safeguard and not disclose my individual authorization to access confidential information (i.e. access code or password). I accept responsibility for all activities undertaken using my individual authorization. Children's can review/audit your access, use, and disclosure of confidential information at any time.
4. I will never post, publish, write or blog (i.e, on social media sites) any confidential Children's information, including pictures, video, or anything which can identify a patient. I will never place patient information on a mobile device (i.e., thumb drive, iPad®, smartphone, tablet, laptop), unless I have appropriate written permission and encryption from Children's. For permission, my Supervisor and the HIPAA Privacy Officer/Risk Manager and HIPAA Security Officer/Divisional Director Information Technology must give prior written permission to me for a limited situation. For encryption, I am responsible to have the Children's issued mobile device encrypted by Children's Information Technology Customer Support. I should contact (205) 638-6568 or gethelp@childrensal.org for assistance. I will not take personal pictures or videos of confidential information. If any mobile device in my possession is connected to Children's email, I am responsible to ensure it is password protected and encrypted. Please refer to the encryption instructions in this policy. By signing this Agreement, I also represent that I have understood, signed, and agreed to the Children's of Alabama Appropriate Electronic Rules of Behavior.
5. I will immediately report activities by any individual or entity that I suspect may compromise the confidentiality and privacy of confidential information, so corrective action can be taken. Reports made in good faith about suspected activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities. I will immediately (requested within 24 hours) report to: My Supervisor; Children's Privacy Officer, (205) 638-5959; Children's HIPAA Security Officer. (205) 638-7878; and/or the anonymous Children's Corporate Compliance Hotline at 1-800-624- 9775 or at the corporate compliance link at www.childrensal.org
6. I understand my obligations under this statement are at any time whether off or on Children's property. My obligations continue after termination of my services with Children's. Upon termination of services, I must not use and must immediately return any originals or copies of any file, document, record, or memorandum relating in any manner to confidential information to my Supervisor.
7. I understand I have no right or ownership interest in any confidential information. Children's may at any time revoke any access or use of confidential information.
8. During the course of performing my services and thereafter, I will safeguard and retain the confidentiality and privacy of confidential information against inappropriate use and/or disclosure at all times. I am responsible if I misuse or wrongfully disclose any confidential information or fail to safeguard my individual authorization to access confidential information.
9. I must wear my business Identification Badge at all times. I understand it must be kept visible, in order to be readable by others, to prove my identity.
10. I understand any inappropriate access, release, or use of confidential information may subject me to disciplinary action (including immediate termination) and/or appropriate legal action, such as prosecution with law enforcement (civil monetary fines and/or imprisonment). I understand my obligations are subject to review, revision, and renewal, as appropriate.

Children's of Alabama
Remote User Policy
July 28, 2008

Reason for this Policy

This policy defines standards for connecting to the Children's of Alabama (COA) network from any remote host. These standards are designed to minimize the potential exposure to COA from damages which may result from unauthorized use of COA resources. Damages include the loss of Sensitive or Restricted Data, including Protected Healthcare Information (PHI); loss of intellectual property; damage to public image; or damage to critical internal systems.

Statement of Policy

Scope:

This policy applies to all Remote Users of COA IT Resources including staff, physicians, residents, outside contractors, vendors, and other agents with a COA-owned or personally-owned computer used to connect to the COA network. This policy applies to remote access connections used to do work on behalf of COA, including but not limited to, connecting to COA resources, reading or sending e-mail and viewing intranet Web resources.

All remote access implementations at COA are covered by this policy including dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, Citrix Access Gateway, and hardware or services provided by third parties.

General

1. It is the responsibility of Remote Users to ensure that all possible measures have been taken to secure the remote machine. This includes hardware and software firewalls and anti-virus software as
2. well as have the most recent operating system and application patches applied. A Remote User's computer system must be at least as secure as its on-site counterpart.
3. Remote Users must comply with federal, state, and local law and all COA policies.
4. All Remote User activity during a remote session is subject to COA policies and may be monitored and logged for compliance.

Requirements

- Secure remote access must be strictly controlled. Access to COA IT Resources will be controlled via either a Cisco VPN Client utilizing a SecurID user account and password or Dial Up Networking also utilizing a SecurID user account and password or through the Citrix Access Gateway utilizing a user ID and password.
- All Remote Users working with Sensitive or Restricted Data must use COA VPN services or the Citrix Access Gateway.
- At no time will a Remote User provide their password to anyone, including family members. COA employees will never ask for a Remote User's password.
- Remote Users must ensure that their COA-owned or personal computer or workstation, which is remotely connected to the COA network, is not connected to any other network at the same time, other than a Private Network under the user's control.
- All hosts that are connected to the COA network must use up to date anti-virus software, keep virus definitions up to date, and run regular scans.
- Remote Users must ensure that systems used to connect to the COA network have the most recent operating system and application patches applied.
- When connecting to the COA network with wireless connections on personal networks, the wireless connections must be encrypted using WEP or other acceptable secure technology. If connecting through a router that has a wireless transmitter, whether connected through either the wired or wireless ports, the transmitter must be configured in an encrypted mode or it must be turned off.
- Users must ensure proper physical security precautions are taken when connecting to the COA network from remote locations. For example:
    A. Machines should not be left unattended while connected or logged into the COA network.
    B. In public environments, users should take precautions to prevent unwanted viewing of computer screens by unauthorized persons.

Risks

Connecting to the COA network from an external source opens up the COA network to any vulnerability that computer may have. If the remote user has viruses, Trojans, or worms running on their computer, those same vulnerabilities can be transferred to the COA network when they connect remotely. Since we will be logging Remote User connectivity, those vulnerabilities will be traced back to their originator.

Compliance

Anyone found to have violated this policy is subject to disciplinary action, up to and including termination.

CHILDREN'S OF ALABAMA

Appropriate Electronic Usage Rules of Behavior

Purpose:

The following Rules of Behavior apply to all users of Children's of Alabama (Children's) information systems regardless of organizational affiliation. These rules are intended to communicate Children's policy in a concise manner and are consistent with policy detailed in approved Children's documents. They do not replace or supersede other policies on the Children's internet/Children's Red Wagon.

Definitions:

Information Systems: An integrated set of components (hardware and/or software) for collecting, storing, processing, and/or communicating information for a specific purpose.

Portable Devices: Equipment capable of processing, storing, or transmitting electronic data designed for mobility. Such devices may interact with other networked systems, the Internet, desktop personal computers via some form of interconnection.

Confidential information: Any information that may only be accessed by authorized personnel. It includes Protected Health Information, financial information, employee data, intellectual property and any information that is deemed confidential or that would negatively affect Children's if inappropriately handled.

Protected Health Information: Protected Health Information **(**PHI) under HIPAA means any information that identifies an individual and relates to at least one of the following: the individuals, past, present, or future physical or mental health, the provision of health care to the individual, the past, present, or future payment for health care. This information is verbal, written, and/or electronic. Information is deemed to identify an individual if any information could enable someone to reasonable determine the individual's identity. **(Caution: even when a name isn't used or it's not a photo of a face, it can still be PHI).**

Phishing: The criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords, and credit card details by pretending to be a trustworthy entity in an electronic communication

System Access & Accountability:

- I understand that my access to Children's information systems is contingent upon my acknowledgement of this Rules of Behavior Form.
- I understand that my user account is equal to my legal signature and I will be responsible and accountable for all work done under this account.
- I understand that I am given access to and will use only those systems for which I require access to perform my official duties/job responsibilities.
- I will not attempt to access systems I am not authorized to access.
- I understand I have no expectation of privacy while using any Children's information system resources and that all my activities are subject to monitoring and auditing.
- I understand that while using Children's information resources that I could represent Children's and I will conduct my business in a professional manner and use good judgment.

Passwords & Other Access Control Measures:

- I will utilize passwords that are at least eight characters long (or as strong as allowed) and use a combination of letters (upper- and lower-case), numbers, and special characters. If the technology does not support such password complexity, I will use the strongest supported password.
- I will protect passwords and other access information from disclosure. I will not provide my password to anyone, including system administrators, my supervisor or management and will not store them on or about workstations, laptop computers, or other devices.
- I will not store authentication devices such as smart cards on or about workstations, laptop computers, or other devices and remove them promptly whenever I leave my work area.
- I will promptly change initial/default passwords or whenever the compromise of my password is known or suspected.
- I will not attempt to bypass access control measures.

Data Protection:

- I understand that I am responsible to protect sensitive information from disclosure to unauthorized persons (those without a need-to-know) in accordance with applicable Children's policies.
- I will not disable or circumvent Children's technical security controls such as encryption, anti-virus, firewalls, monitoring and administrative tools. I will cooperate with software updates, downtime, and other communications from Customer Support. I will not respond to any "phishing attempts," where a criminal is intending to be a real company and gain your identifying information. This may be communication that you did not request (i.e. from a "bank"). Please forward any phishing attempts to Customer Support.
- I will not transfer sensitive information to an unencrypted and un-approved device.

- I understand that I have a responsibility to close or log off applications after use.
- I will not access, process, or store sensitive information on non-Children's equipment such as personally owned computers unless properly authorized to do so.

Internet & E-mail Use:

- I understand that my Internet and e-mail is for official use, with only limited personal use allowed.
- I will only use my Children's email for business use. I will not forward information from my Children's email to other accounts (@hotmail, @gmail) to conduct business.
- I will not use public e-mail, chat or other Internet-based communication systems (e.g. AOL, Gmail, Yahoo, Hotmail, iCloud) to communicate sensitive information.
- I will not use "peer-to-peer" file sharing, "Internet Cloud", web proxy or Internet-based backup web sites and will consult with Children's Information Technology Customer Support, (205) 638-6568; gethelp@childrensal.org for approved methods.
- I will not provide personal or official Children's information solicited by unknown individuals or suspected phishing e-mail or web sites.
- I will not distribute non-business mass mailings, viral e-mails or other spam to fellow e-mail users.
- Avoid emailing PHI when possible. If I must send an email outside Children's firewall (childrensal.org or peds.uab.edu), I am required to encrypt the message. To encrypt an email, first correctly spell private in the subject line. Second, you will get an email with a password that needs to be forwarded to the recipient of the encrypted message so they can open the email. If you are emailing a patient/parent please be sure a patient/parent email consent form is on file. Contact the Privacy Officer with questions.
- I will not email psychiatric information or anything with a sensitive diagnosis (HIV/AIDS, abuse). This information has an extra level of sensitivity under Alabama state law, as well as federal HIPAA law.

Software:

- I agree to comply with all applicable software licenses and copyrights.
- I will not install non-standard software on Children's equipment without prior approval from Children's Customer Support. This includes software available for download from the Internet, the Children's web site, and personally owned software.

Use of Children's Equipment:

- I understand that Children's equipment is to be used for official Children's use, with only limited/incidental personal use as approved by my supervisor on the condition that it does not interfere with my job, deny others access to Children's information systems, consume significant information system resources, and does not result in significant cost, legal or regulatory risk to Children's. Examples of unacceptable use include, processing obscene, harassing, or unlawful material, large personal video/audio/photo librari.es, excessive couponing, copyright infringements, etc.

Laptop Computers & Portable Devices:

- I understand that any laptop computers and portable device used for Children's business and/or connected to Children's email must be password-protected and encrypted using Children's approved encryption methods**.**
- Contact Information Technology Customer Support at (205) 638-6568; gethelp@childrensal.org.

If you purchase a laptop computer & portable device (smartphone, thumb drive) for Children's business use, you must have prior written approval of the purchase from your Supervisor and contact Customer Support to help ensure the device has appropriate password and encryption settings.

- I will not disable any Children's software or security controls unless I am directed to do so by Children's Customer Support.
- I will use my laptop computer & portable device to take any photography/videos/other images of Children's confidential information (including pictures of patients and other employees), unless approved in writing from Corporate Communications.
- I understand that such activities require specific documentation and/or approval and violations may result in disciplinary consequences.

Wireless Networking: New wireless systems used for Children's business must be approved by the Chief Information Officer Divisional Director, Information Technology and HIPAA Security.

- Wireless systems not compliant with minimum-security controls or Information Technology recommendations are absolutely prohibited and subject to immediate disabling and confiscation of hardware.
- Requests for connectivity to the wireless networks shall be approved by Information Technology.
- I should avoid the use of guest/public wireless systems for business/patient care.

Telecommuting (travel, home or satellite office):

- I will follow the same HIPAA and confidentiality policies as those required of me at work when I am telecommuting.

- I will properly dispose of media containing sensitive information in accordance to Children's policy and procedure. For instance, paper confidential information when appropriate to dispose of must be placed in the approved official shredding bins at Children's (Document Destruction). For electronic media, contact Customer Support for assistance.
- I understand I am absolutely prohibited from removing charts or copies of Protected Health Information from Children's campus. If your supervisor allows you to do handle PHI electronically, you are responsible to absolutely ensure it is encrypted.
- I understand that if Children's determines a portable media devices contains PHI or ePHI and it is lost or stolen, I must agree to remotely swipe the device. This will cause loss of all the data in the device.

Incident Reporting and Contacting:

- I will report Information Technology incidents to Customer Support as soon as I become aware of the incident. (205) 638-6568; gethelp@childrens.org

Sanctions:

I acknowledge that I have read these Appropriate Electronic Usage Rules of Behavior, I understand them, and I will comply with them. I understand that failure to comply with these rules as well as any applicable Children's policies, standards, procedures, security controls or regulations could result in disciplinary action against me, up to removal of system access and immediate dismissal. In accordance with the HIPAA/HITECH and HIPAA Omnibus, there could also be a lawsuit against me for fines/money or criminal prosecution (jail time). These rules also apply to me upon termination of my services.