|  |
| --- |
| **Requestor Information** |
| **DEPARTMENT:** |  |  |  |
| First Name | MI | Last Name  | Job Title |
| Address  |  |
| Phone Number | E-mail Address  |
| [ ]  Tribal Employee | [ ]  Contractor Company | End date: |
|  |
| **Type of Employment** |
| [ ]  Full Time | [ ]  Part Time |  | [ ]  Temporary | [ ]  Volunteer |
|  |
| **Systems** I am requesting access to the following information systems |
|  |  |
| [ ]  ADMIN  | [ ]  TIMECLOCK |
| [ ]  ABILA /MIP |
|  |  |
|  |  |
| [ ]  RPMS | **Last 4 digits of SSN:** (if user requires access to patient data) |
|  | [ ]  Physician [ ]  FNP [ ]  Dentist  |
| **ROLE** | **ACCESS NEEDED OR MIMIC CURRENT USER:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
|  [ ]  RECEPTION | [ ]  Scheduling [ ]  Patient Registration [ ]  Vista Imaging |
|  [ ]  BH | [ ]  Staff Psychologist [ ]  Mental Health counselors  |
|  | [ ]  Social Workers [ ]  Alcohol & Subst. Abuse Counselor |
|  [ ]  DIABETES | [ ]  DM GUI [ ]  Registries LIST POSITION:  |
|  [ ]  CHR |  |
|  [ ]  DENTAL | [ ]  DENTRIX user |
|  [ ]  BILLING | [ ]  Coder [ ]  Biller [ ]  Claims [ ]  AR [ ]  AR Supervisor |
|  [ ]  MED REC | [ ]  Technician [ ]  MED REC Supervisor [ ]  Coder [ ]  Data Entry  |
|  | [ ]  Correct Medical Records [ ]  Vista Imaging Scan [ ]  Scan Supervisor |
|  | [ ]  Patient Sensitive Tracking [ ]  Patient Flag Package Manager |
|  [ ]  ADDITIONAL | [ ]  ICARE [ ]  CRS [ ]  IMMUNIZATION Coordinator [ ]  ROI  |
|  |  |
|  [ ]  CHS RCIS | [ ]  SUPERVISOR [ ]  CHS [ ]  CHS SUPERVISOR TAXONOMY (FP, Int, Ped, etc.): |
|  [ ]  RADIOLOGY | [ ]  TECHNICIAN [ ]  STAFF RADIOLOGY 1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  |
|  [ ]  LAB | [ ]  TECHNICIAN [ ]  PHLEBOTOMISTS 2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  |
|  [ ]  ADDITIONAL | State License No. : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ State: \_\_\_\_\_\_ |
|  LIST | NPI #: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ SPI #: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Provider Classification or Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Copy of DEA card must be attached: #\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Virtual Private Network (VPN)/Firewall (FW)** |
| **[ ]  VPN ACCESS** | **Provide 2 Telephone Numbers** |  | **justification** |

 Supervisor Signature Date Network Access Granted BY: Date

**\*\* The Rules of Behavior (RoBs) and the General User Security Handbook are posted on K’ima:w Medical Center’s Intranet Page (http://10.248.14.28/)**

The Rules of Behavior (RoBs) and the General User Security Handbook (SOP 06-11a) shall be provided to all users requesting access to IHS/KMC information and information systems. Access to any IHS/KMC systems shall not be granted without appropriate completion of the Information Technology Access Control (ITAC) form and Receipt of Rules of Behavior at the time of initial access request and annually thereafter.

All government staff, contractors, and other users of IHS/KMC systems are required to read the RoBs and are responsible for abiding by its contents. Signing the Receipt of RoBs and the ITAC acknowledges the user understands of the requirements for access to IHS/KMC information and information systems and their individual responsibilities as a user.

**I certify that I have read the IHS rules of Behavior for Information Technology Users in its entirety, and understand and agree to comply with its provisions. I understand that violations of the IHS/KMC rules or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities. I understand that exceptions to the IHS Rules must be authorized in advance in writing by the IHS Chief Information Officer (CIO) or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 19 USC 2071, which the IHS Rules draw upon, can result in monetary fines and/or criminal charges that my result in imprisonment.**

**Signatures:**

Employees/User’s Signature Printed Name Department Date

* Access to the above systems is required in the performance of my official duties. I shall protect the information in accordance with all Public Laws and Agency regulations. I understand I am subject to criminal and civil penalties prescribed by law for any violations thereof.
* I have received, read, understand and will abide by the IHS Rules of Behavior provided with the access request form and any system specific rules of behavior provided to me at a later date pertaining to the above access request.
* I have an obligation to protect any information which the loss, misuse, unauthorized access to, or modification of could adversely affect the conduct of federal programs. (*Information about individuals, especially personally identifiable information (PII) is confidential and protected from unauthorized disclosure by law and regulations. Improper access to, or unauthorized disclosure of data through a computer or otherwise is subject to the imposition of criminal penalties and/or disciplinary action)*
* I understand that my obligation to protect IHS/KMC data from unauthorized disclosure does not end with either the termination of my access to this system or with the termination of my government employment /contract.
* I will safeguard the passwords. (e.g. access codes, verify codes) given to me. I may use my passwords only in the performance of my official duties. I may not disclose my passwords to anyone for any reason. I am accountable for all work performed or changes made to the system/databases under my passwords. I will not allow anyone else to access any of the above designated information systems, or through them, to any other information system. Using my passwords.
* I understand that electronic mail/Intranet/Internet access on any government systems is to be used for official government business only. This applies to access reached through any of the above-designated systems. It is understood that the Information Security Officer and network/systems administrators may monitor electronic mail and Internet/Intranet traffic, including the contents of messages and downloads of information.
* I understand that I may have disciplinary or adverse action taken against me and may be prosecuted if I use electronic mail, computer hardware/software or Internet/Intranet access for any purpose other than performance of IHS/KMC business in fulfillment of my official duties except as outline in the IHS guideline, “Policy on Limited Personal Use of Government Office Equipment Including Information Technology”.

**I affirm with my signature that I have read, understand, and agree to fulfill the provisions of this notice. I will complete the IHS Security awareness training within 24 hours of receiving access (unless I have read the HHS Quick Guide to Information Security in which case I will have 30 days to complete the training) or my access will be revoked until training is completed.**

**The website address is:** [**www.ihs.gov/issa**](http://www.ihs.gov/issa)

**User’s Signature Printed Name Telephone Date**

**Supervisor Approval Printed Name Telephone Date**

**Facility Approving Official & Title Printed Name Telephone Date**

**Annual Review**

 **I have reviewed this user’s computer access and determined the current level of access is appropriate.**

**Supervisors Signature: Date of Review**

**User’s Signature: Date of Review**