New Mexico Health Care Authority - Security Access Form

INSTRUCTIONS

1. CHECK ONE - Check off the appropriate action to be completed.
2. USER INFORMATION – ***Print all the following:***
   Name (last, first, MI), Work Phone, Fax Number, Date the form is being completed, Work Location – Building and address, SHARE Employee ID if existing employee, Working Title – Employee's job or position title, Division/Bureau/Contractor – Division and Bureau names. If a Contractor, name of the firm representing the contracted employee.
3. Contact Person – Name of Person to contact if any questions arise for requested SAR
4. MIRROR ACCESS - Please provide the name of someone who has the access this new or transferring user has so that we can ensure they have all systems and access needed for job title.
5. STANDARD ACCESS- Check off the systems the employee is to have access to. State employees have standard access to certain systems unless noted.
   Note on Server/Drive Access: Please provide the drive as its shown on another users PC. If needed you can attach a screenshot of the drives screen. If you put only a letter (ex: N:) this does not provide detail needed to provide requested access.
   Website Access - Access to HCA web applications, and other websites belonging to other Agencies
   ASPEN / Yes NM- Access to ASPEN and Yes New Mexico Portal. **Please note, for proper ASPEN access, name, phone number, primary office, job title, gender, supervisor, and manager must be provided on the form**
6. APPLICATION ACCESS-
   Check the systems you are requesting access.
   NOTE: Access to certain systems is based on the employee's working title and division. Each division/bureau has employees with pre-defined access. Production Control has a list of working titles with defined access.
7. DOMAIN ACCESS -Access to other systems belonging to other divisions requires approval from the Directors of those specific divisions. Used by DoIT staff members and pre-approved employees or contractors. If VPN access is requested, the justification section must be completed and approved by the HCA CIO. Admin Access needs approval from the CIO. These programs are used by DoIT staff/contractors.
8. AGREEMENTS- **Employees/Contractors** must read the "Health Care Authority Security Code of Conduct" and "Executive Branch Information Technology Resources" policies, and by signing the security form they acknowledge and understand the consequences if they violate either one.
9. APPROVALS
   a. ***Print*** and ***sign*** your name in the fields provided.
   b. Date you signed the form.
   c. System access must be authorized by your direct supervisor. Certain access must also be approved by appropriate higher-level management.
   d. Name of the contact person to notify when Production Control has completed the request.
   e. Title
   f. E-mail Address
   g. Phone Number
10. BUSINESS PROCESS-
    a. The Security Access Form must be faxed or emailed to Production Support at 827-9416 or HCA-NetworkHelpDesk@hca.nm.gov. Security access form may also be completed or loaded into Cherwell Self Service Portal and ticket will be generated for Production Support as well.
    b. Production Support will verify all the appropriate signatures on the form.
    c. To grant access to ASPEN the form will be sent to ASPEN Helpdesk via Cherwell for completion.
    d. Production Support will grant the access requested on the form and email will be sent with all logins and ASPEN ticket number

HEALTH CARE AUTHORITY

New Mexico Health Care Authority Division of Information Technology Security Access Request
Fax – 827-9416 (Fax pages 3 & 4 only)
Send To: HCA-NetworkHelpDesk@hca.nm.gov
Submission: http://charger/CherwellPortal/ITSelfServicePortal

Processing time of a form can take up to 2 weeks from the date received so please submit all forms as early as possible.

EMPLOYEE INFORMATION

Last Name	First Name	MI	Work Phone	Date

Work Location & Address	SHARE Employee ID (if existing)	Working Title	Division/Bureau ☐ Contractor ☐

(3) Contact Person (If Questions Arise)

Name and Phone Number	Title	Requested Date for Changes

SELECT SAR REQUEST

Add New User

Access Removal Request

Employee Status Transfer ☐ **Disabled All Access** ☐ **Disable Application Access:** SELECT ONE ☐ **Remove network share access** _____

Computer Login (AD) and Email Access Request

MIRROR SYSTEM ACCESS OF EMPLOYEE : _____

Domain Access: ☐ NT – Network \ Outlook Access ☐ Server/Directory Drive- ☐ Modify Access (Please list drive as it is on PC not just letter) _____

Supervisor Signature Required Apps: ☐ MS Project ☐ MS Visio ☐ Power BI ☐ Accellion Encrypted Email (Fee $17.25)

☐ **SSL VPN /RSA/TOKEN** **VPN Approved: Yes** ○ **No** ○ **Expiration Date**: **HSD CIO/CSO Signature**:

Application Access Request

☐ **FIS \ EBT** ☐ **UI** ☐ **OMNICAID** ☐ **VOSS**

☐ CTS *Supervisor:* ☐ **JAMA** ☐ **JIRA** ☐ **Cherwell** ☐ **Medicaid Web Portal**

Sharepoint Access

☐ **Sharepoint:** Choose One Choose One Specify URL link if known: _____ ☐ **DWS-** Access to DOL Wage Verification -Inquiry Only _____ (***SHARE ID Req***)

ASPEN and YNM Access

☐ ASPEN Gender Male *Supervisor:* _____ Role/Office needed if other than job title: _____

☐ SAVE ☐ MVD Work # _____ ☐ **Yes NM** _____ Please list roles need _____ ☐ ASPEN BI _____ **(Region)**

SALESFORCE Access

Replacement Supervisor, if so please name the predecessor? My Teams Task Group

☐ SALESFORCE *Supervisor:* _____ SWQ Access Type Non Supervisor Role User Type: Case Worker _____

Equipment Request

☐ **Laptop** ☐ **iPhone** ☐ **Keyboard/Mouse** ☐ **Monitor** 1 ☐ **ID Badge** ☐ **Docking Station** **DOIT CODE :**

☐ **OTHER** : Please specify ANY other access needed not listed in SAR

(8) AGREEMENTS

EXECUTIVE BRANCH CODE OF CONDUCT Section 4 USE OF STATE INFORMATION TECHNOLOGY RESOURCES
And **HEALTH CARE AUTHORITY CODE OF CONDUCT, Section 041.8 "DISCLOSURE OR MISUSE OF CONFIDENTIAL OR OFFICIAL INFORMATION":**

41.8.1 Prohibited by Law An employee may not disclose confidential or official information if the disclosure of such information is prohibited by law or regulation or would be contrary to the best interests of the department or its clients. This includes protected health information covered under HIPAA. This also includes confidential information from other governmental agencies.

41.8.2 Private Gain An employee may not disclose or misuse confidential or official information not generally available to the public, or acquired by virtue of his/her employment with HCA, for his/her own or another's private gain. This includes any information regarding awarding contracts or grants by the department before the official release of such information.

I, the Employee/Contractor have read the HCA Code of Conduct Section 041.8 and the Executive Order, Code of Conduct Section 4 Use of State Information Technology Resources. I fully understand the terms of these policies and agree to abide by them. I realize that the Health Care Authority's security software may record for management use the internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I know that any violation of this policy could lead to dismissal or criminal prosecution.

I, the Employee/Contractor understand that the Health Care Authority's electronic mail system is the Health Care Authority and State property and intended to be used primarily for business purposes. I understand that excessive use of the E-mail system for the conduct of personal business is strictly prohibited. I acknowledge that any message I send or receive may be recorded and stored in an archive file for management use.

I, the Employee/Contractor understand that the Health Care Authority reserves the right to access, review, and disclose information obtained through the E-mail system at any time, with or without advance notice to me and with or without my consent. I know that any violation of this policy could lead to dismissal or criminal prosecution.

I, the Employee/Contractor confirm that I have read the acknowledgment and have had an opportunity to ask questions about it. I also agree to abide by the terms of the HCA Code of Conduct and the Executive Branch Code of Conduct, Use of State Information Technology Resources. .

By signing this Security Request Form, the **Employee/Contractor** agrees to be held to the same standards as HSD Employees as per the HEALTH CARE AUTHORITY CODE OF CONDUCT, PARAGRAPH 041.8, "DISCLOSURE OR MISUSE OF CONFIDENTIAL OR OFFICIAL INFORMATION." Signatures or references to Employee in this document will also refer or apply to HCA Contractors.

(9) APPROVALS (SAR approval cannot be authorized by person who is getting requested access it must have supervisors signature)

	Name (Please Print)	Signature	Date	Phone	Email Address
Employee					
Supervisor					
Bureau Chief/ROM					
Deputy Director					
Director/CIO/CSO	REQUIRED FOR VPN ACCESS				

(10) ITD USE ONLY:

Name of Security Technician (Print)	Name of Security Technician (Signature)	Date
Name of System Admin (Print)	Name of System Admin (Signature)	Date