New Jersey Department of Human Services
Division of Aging Services

ACCESS REQUEST FORM FOR SALESFORCE GOVERNMENT CLOUD
Acute Care Provider EARC User

Request Type: ☐ New ☐ Update **Date:** _____

Section A: To be completed by the person requesting access

First Name: _____ MI: _____ Last Name: _____

Mother's Maiden Name: _____ Work Phone #: _____

Work E-Mail: _____

I have read the Computer User Responsibility Acknowledgement on pg. 2 of this form and agree to comply.

Signature: _____

Date: _____

Section B: To reinstate login

Disabled User ID: _____

Section C: To be completed by the supervisor

Provider: _____

Street: _____

City: _____ State: _____ Zip Code: _____

First Name: _____ MI: _____ Last Name: _____

Title: _____ Work Phone #: _____

Supervisor Work E-Mail: _____ Work Fax #: _____

Supervisor Signature: _____ Date: _____

ISR Name: _____

ISR Signature: _____ Date: _____

Computer User Responsibility Acknowledgement

Government agencies have a particular responsibility to maintain the confidentiality and accuracy of the data that is stored in its computer and electronic systems. The Division of Aging Services (DoAS) will enforce a policy of individual user responsibility for access to and use of its information and systems.

Users must notify DoAS immediately if they have left the provider organization or if any contact information has changed. Users must contact DoAS at EARCRegistration@dhs.state.nj.us.

Users shall stay current with updates to the EARC process by checking the website at www.state.nj.us/humanservices/doas.

Users shall use the online EARC system approved by DoAS, which administers the EARC process.

Users shall help ensure the EARC is completed as truthfully and accurately as possible.

Users shall adhere to the requirements of all applicable state and federal laws, rules, and regulations pertaining to the confidentiality and disclosure of information and records. All consumer/applicant information must be kept confidential under federal and state law. Users shall not give information to anyone unless requested by the consumer/applicant.

Users must use appropriate safeguards to prevent the disclosure of consumer/applicant protected health information and other consumer/applicant personal information. Users also shall protect against reasonably anticipated threats to confidentiality. Users shall ensure that consumer/applicant information is kept confidential and is stored in a secure location. All information that is no longer needed by the provider organization shall be shredded. Users shall follow the comprehensive information privacy and security program of their provider organization.

Users must notify DoAS immediately in the event of an improper disclosure of consumer/applicant protected health information or other personal information. In such event, users must contact DoAS at 609-588-6675.

In addition, by signing this form, I acknowledge that I understand the following Computer User Responsibilities:

- Computer system passwords are assigned to each individual computer user for that individual's use only.
- Computer system passwords must be kept confidential by the assigned individual. Passwords are not to be shared with anyone, including supervisors.
- Use of computer systems shall be limited to YOUR job-related duties only.
- Computer users must sign-off (log-off) from password protected computer systems if they are not physically present. Personal computer users may activate a confidential password-protected screensaver.
- Computer users that fail to adequately protect their logins, passwords and confidential data from inappropriate disclosure/use/theft are personally liable for any potential consequences.

User accounts not used for 60 days will be automatically deleted from the system. A User whose account was deleted will need to submit a new Access Request Form to regain access.

DoAS reserves the right to revoke a User's account for breach of this agreement.