Frequently Asked Questions About
Updated Language in CSOSA Contracts

Personnel Security Requirements

My company has been doing business with CSOSA for years with no background investigations. Why is a background investigation required now?

After reviewing the Agency's contract personnel security requirements, the Office of Security has determined that contractors with certain responsibilities must undergo "CSOSA background checks" and/or an "Office of Personnel Management (OPM) background investigation." There are three primary reasons a background check is conducted:

- Access to physical agency facility
- Access to Agency network/information systems
- Risk or exposure to Agency (e.g. information, sharing, disclosure, etc.)

After the CSOSA background check or OPM background investigation is successfully completed, what level of clearance will the employee hold?

CSOSA's background check clears a contractor's employee to perform the work stated in the contract. However, after approval the contractor's employee will not hold any National Security Clearance (for example, Secret or Top Secret). CSOSA does not handle national security matters; therefore, CSOSA does not issue "clearances" for contractors or their employees.

How long does a CSOSA background check take for approval and will it delay the start of the contract?

It depends on the type of investigation and issues that arise. Contractor employees may not start work on CSOSA services until the Office of Security has conducted "background checks" and issued a security approval. Contractors should allow up to 30 days from submission of properly completed forms.

Where do I get the forms my employees need to complete for the CSOSA background check and if necessary, the OPM background investigation Investigation?

The Contracting Officer (CO) or Contracting Officer Representative (COR) will provide the security forms, as appropriate. If it is determined that the contractor will be working longer than 180 days the Office of Security will provide the additional security forms that are required for the OPM background investigation.

How long do the employees have to complete the security forms?

Contractors should allow up to 30 days prior to the required start date for the CSOSA background check. Delays in submitting the security forms will result in delays of authorization to begin work.

What happens if one of my employees refuses to provide sensitive information such as the credit release or fingerprint cards?

The employee will not be approved to start work on CSOSA services.

Are there any special procedures I have to follow under this contract clause if one of my employees working on the contract is fired or resigns?

If a contractor employee is fired or resigns the contractor must notify the COR immediately.

Upon security approval, when will my employees receive CSOSA-issued identification badges?

Once the Office of Security has completed the background checks and renders security approval, the contractor employee will be eligible to receive an identification card if needed to perform contracted functions.

Do my employees require identification cards to begin work at a CSOSA facility?

If unescorted physical access to CSOSA facilities is required to perform contract services, then a CSOSA-issued identification card will be issued.

If an employee is denied security approval after the CSOSA background check or the OPM background investigation, is there any right to appeal the determination?

There are no appeal rights.

I have some employees that provide indirect services under the CSOSA contract. Do I need to submit these workers for background approval as well? If so, what is the process and who decides which of my employees need to be submitted and which do not?

You should contact your COR with this inquiry. The COR will in turn contact the Office of Security for technical review and guidance. Through review and contact with the COR, the Office of Security will decide whether a contract employee performing indirect support shall be subject to CSOSA background approval.

Information Security Requirements

What is Personally Identifiable Information (PII)?

The term "PII," refers to any information that alone can be used to distinguish or trace an individual's identity, such as a name, social security number, and any biometric identifier, or information that when combined with other personal or identifying information, such as hair color, date and place of birth, and mother's maiden name, can be linked to a specific individual.

Under previous CSOSA contracts, my firm has been allowed to store PII about CSOSA staff, offenders and/or clients on our own computer system. Does this provision mean we can't do that anymore?

You can no longer store PII on your own computer system because the risk of unauthorized access and misuse of PII is greater.

Why is this requirement being imposed?

In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974, contractor access to CSOSA information and information systems must be maintained at the highest level of protection in order to thwart unauthorized disclosure of sensitive information. The requirements apply to all CSOSA contracted services and information resources located and operated at contract facilities, at other government agencies that support CSOSA mission requirements, or any other third party using CSOSA information in order to perform a CSOSA authorized activity. These requirements also apply to all contracts in which CSOSA information is used, stored, generated, transmitted, or exchanged by CSOSA, a contractor, subcontractor or a third party, or on behalf of any of these entities, regardless of format (e.g., paper, microfiche, electronic or magnetic portable media) or whether it resides on a CSOSA owned system or a contractor's system operating for or on behalf of CSOSA.

I was told my office computer systems are not "FISMA" compliant. What does that mean?

The Federal Information Security Management Act of 2002 (FISMA) requires an extremely comprehensive set of management, operational, and technical controls be implemented to guard against unauthorized access, use, disclosure, disruption, modification, or destruction and to protect the integrity, confidentiality and availability of systems and information.

Unless your organization has followed the guidance detailed under the National Institute of Standards and Technology's Special Publication 800-37, Applying Risk Management to Information Systems, and have implemented and are managing information security risk in accordance with SP 800-37 and all of the supporting NIST guidance, it is highly unlikely that your computing environment is "FISMA Compliant".

How will my staff obtain access to the CSOSA network server to review or add information?

Your COR will provide you with a Computer Access form to complete and sign. You will be notified when CSOSA's Office of Information Technology has approved access.

My company uses Cloud storage for our data. Is this prohibited under this contract provision?

This must be approved in writing and the cloud storage must meet FISMA requirements as well. This is accomplished through a federal certification program. The Federal government has established the Federal Risk and Authorization Management Program (FedRAMP) for certification of service providers such as a cloud storage service providers. To learn more and whether a service provider is certified, you may visit FedRamp.

The only PII we obtain from offenders and/or clients is their name, PDID and Social Security Number. Does this contract provision still apply?

Yes. Name, PPID, and/or SSN is stand-alone information that can be used to distinguish or trace an individual's identity. Therefore, this information must be protected from unauthorized disclosure. PII must only be seen by those authorized to see it, heard by those authorized to hear it, and sent to those authorized to receive it.

Does this contract provision still apply to paper files as well as electronic records?

Yes. Records come in all media, such as paper, electronic (including e-mail), and voicemail, to name a few, and the format of the information is irrelevant. The contract provision applies regardless of whether the file is stored in traditional containers such as file cabinets and boxes, or on a network server, desktop, laptop, handheld, or other device with text or instant messaging capability.

We have updated our system and believe we have adequate information security. Can we get an exception to this contract provision? If so, how?

You must provide evidence that your organization has institutionalized a risk management process that includes security categorization, control implementation, assessment, and authorization that is consistent with NIST SP 800-37.

Why do I have to report a breach, loss or unauthorized disclosure of data within one hour of its discovery? Who do I report the incident to?

The Office of Management and Budget Directive M-01-16 and CSOSA policy requires the reporting of incidents involving breaches of PII within one hour. . The incident should be reported to the COR.

Records Management Requirements

The CSOSA contract with my company contains new language about complying with all Federal records laws. Why am I being asked to do this now?

The creation and maintenance of complete and accurate records are basic aspects of records management. Based in statute, the practice of ensuring "adequate and proper documentation" contributes to efficient and economical agency operations by guaranteeing that information is documented in official files, including electronic recordkeeping systems, where it will be accessible to all authorized staff that may have access to the information.

How do I find out what the Federal records laws and regulations require?
Information on Federal records laws and regulations can be found at:

- 44 U.S.C. Chapter 31 and 44 CFR Chapter 31 (Records Management by Federal Agencies)

- 44 U.S.C. Chapter 33 and 44 CFR Chapter 33 (Disposal of Records)

The contract provision refers to information covered by the Privacy Act of 1974 or the Freedom of Information Act. What kind of information is covered by these two laws?

The Privacy Act of 1974 provides privacy protections for personal information maintained by federal agencies and applies to all federal agencies, including CSOSA. The Act provides privacy protections for personal information that agencies collect, maintain, use or disseminate in a "system of records." The type of records covered is any item, collection, or grouping of information about an individual such as education, financial transactions, medical history, and criminal or employment history and that contains the name, or the identifying number, symbol, or other identifier assigned to the individual, such as a finger or voice print or a photograph.

The Freedom of Information Act (FOIA) provides the public with a right of access to records (hard copy and electronic), that are maintained by federal agencies, including CSOSA. Any person can request records under FOIA; however, certain exemptions permit the withholding of certain information.

Do these requirements extend to emails that have content related to the services we are providing under the CSOSA contract?

Yes, contractors shall treat all deliverables under the contract as the property of the U.S. Government for which CSOSA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.

We don't keep paper records – everything is electronic. Does this contract provision still apply?

Yes. Whether a record is in paper or electronic format does not determine its value or retention period; its content is the key factor, CSOSA owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

In the past, my company has retained treatment records on the offenders and/or clients referred by CSOSA under our contract. Can we still do this?

No, CSOSA owns the rights to all data/records produced as part of the contract. This means that closed treatment records are retained by CSOSA at the end of each year and all remaining records are retained at the completion of the contract. In addition, CSOSA has the right to inspect and access records at any time. Written justification must be submitted to the agency with supporting guidance to maintain a copy of the file. Once reviewed, a decision will be provided in writing to the vendor.

Why can't we simply shred all sensitive documents created under the contract when the performance period is completed?

The disposition of both temporary and permanent records requires the prior authorization of CSOSA Records Manager. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701.

We may need to bring in subcontractors to handle an unexpected volume of referrals under the CSOSA contract. Can we do this under this contract provision?

Yes; however, the subcontractor is held to the same standard as the prime contractor and the prime contractor is responsible for ensuring the subcontractor complies with all contract requirements.

File Maintenance Requirements

Our staff sometimes takes client files home or back to our office to complete weekly progress notes or monthly progress reports. Is this practice allowed under this contract provision?

At CSOSA, we are committed to preserving the privacy and confidentiality of sensitive information. Our goal is to uphold the trust and confidence that our clients place in us. All medical records and documents containing PII must be adequately secured to help ensure our clients' information is not exposed to unauthorized individuals. Therefore, do not remove client files from your office without the prior written approval of CSOSA.

All of our files are electronic. How am I supposed to separate CSOSA and non-CSOSA patient files?

CSOSA files are to be separated in identifiable file folders with unique codes that separate the records from any other business files. The data should be easily identifiable and retrievable within the electronic system to identify CSOSA records.

We have our own internal policy about how a treatment file must be organized and maintained. Are we allowed to substitute this policy for the CSOSA contract provision on file maintenance?

No, as stated within the contract you agree to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.].

Different staff members may treat the CSOSA-referred offender/client over the course of treatment. Do we need to have signed waivers of confidentiality from the offender/client for each staff member treating the CSOSA-referred offender/client?

No, a new waiver does not need to be signed for each staff member treating the CSOSA-referred offender/client. However, when you subcontract out any part of the treatment, a waiver must be signed by the CSOSA-referred offender/client and the subcontractor.

We provide counseling services at a CSOSA facility but maintain the treatment files at our offices. Is this permissible?

No, as stated in the contract you shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.