Privacy Technical Assistance Center

For more information, please visit the Privacy Technical Assistance Center: www.ed.gov/ptac

Identity Authentication Best Practices

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on www.ed.gov/ptac.

Purpose

There is an increasing demand for access to education data, as state and local educational agencies build robust education data systems to facilitate the management and sharing of student records. Educational organizations are legally and ethically responsible for protecting the privacy and security of education data they collect, store, and utilize. In order to ensure that only appropriate individuals and entities have access to education records, organizations must implement various forms of authentication to establish the identity of the requester of the information with a level of certainty that is commensurate with the sensitivity of the data. This process involves identifying and validating the identity of the requesting entity with the required degree of confidence that he or she is who that person claims to be. To help organizations manage access to education data, this brief offers best practice suggestions for developing and implementing effective authentication processes. General recommendations outlined below apply to all modes of data access, be it in person, over the phone, by mail, or electronically. Please see the Glossary for definitions of technical terms.

Using reasonable methods to authenticate the identity of parties to whom educational agencies and institutions disclose education records, as required by the Family Educational Rights and Privacy Act (FERPA), will help educational agencies and institutions improve the transparency and availability of education data while protecting the privacy and security of education records by increasing the effectiveness of access controls.

NOTE: *FERPA regulations require parents or eligible students to provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information (PII) from education records, except as provided in §99.31 of the regulations (34 CFR §99.30). Further, the FERPA regulations require educational agencies and institutions to* ***use reasonable methods to identify and authenticate the identity of parents, students, school officials, and other parties before disclosing or permitting access to PII*** *(34 CFR §99.31[c]). These requirements help to ensure that educational*

agencies and institutions protect the privacy of education records and do not violate FERPA by disclosing education records to the wrong party.

Additional information may be found in the preamble to the December 9, 2008 FERPA regulations amendment at 73 Fed. Reg. 74806, 74840-74841 (link provided below in Additional Resources Section).

The authentication methods discussed in this guidance document are intended to serve as examples of best practices, and the provided list of methods should not be considered to be exhaustive. Alternative identity authentication methods are available, and new methods are being developed on an ongoing basis. As technology and data security standards change, organizations should regularly review and update their procedures to ensure that they continue to use reasonable methods to authenticate the identity of all parties before disclosing PII.

What is Identity Authentication?

"Authentication of identity" means ensuring that the recipient of education records or the party who receives or transmits students' records is, in fact, the authorized or intended recipient or sender. Authentication is the process by which an educational agency or institution establishes the appropriate level of identity authentication assurance, or confidence in the identity of the person or entity requesting access to the records. This assurance is established through the use of a variety of vetting methodologies, which employ so-called "authentication factors," individually or in concert, to raise the level of confidence that the party being granted access is the person or entity it claims to be.

Requirements for specific authentication factors or their combination may vary depending on the type of education records being accessed (e.g., more or less sensitive) and the way in which they are accessed (e.g., in person or electronically). However, the same degree of certainty in the requester's identity should be required for access to data of the same sensitivity level. This means that although educational agencies and institutions most commonly provide access to education records by computer or telephone, they must have procedures in place to be able to establish the same level of identity authentication assurance regardless of whether the data are accessed via electronic systems, mail, fax, telephone, or in person.

What are Authentication Factors?

Typically, an individual's identity is authenticated through the use of one or more factors, such as a Personal Identification Number (PIN), password, or some other factor known or possessed only by the authorized user. Single-factor authentication requires a user to confirm identity with a single factor, such as a PIN; an answer to a security question; or a fingerprint. Two-factor and multifactor approaches require the use of two or more methods to authenticate an individual's identity. For example, in addition to the PIN, a user has to provide an ID card and/or have a matching iris pattern. Authentication factors fall into several categories:

Knowledge Factors (something the user knows): The requesting party demonstrates that it has knowledge of some unique data associated with the party whose identity is being authenticated, such as a *password*, *security questions*, or a *PIN*.

Ownership Factors (something the user has): The requesting party demonstrates that it has possession of something uniquely associated with the party whose identity is being authenticated, such as a *security token* (see Glossary for definition), *email account*, *ID card*, or a *mobile device* (in the case of a mobile device, ownership can be confirmed by sending a one-time password to the device that has been pre-registered with the organization).

Inherence Factors (something the user is or does): The requesting party demonstrates that it has a feature inherent to the party whose identity is being authenticated, such as a matching *fingerprint*, *iris pattern*, or *facial features* (these techniques are commonly referred to as "biometrics").

The choice of the specific authentication method often varies depending on the level of sensitivity of the data that are being disclosed. For example, an organization may determine that a single-factor identity authentication, such as using a standard format username combined with a secret PIN or password, is reasonable for protecting access to student attendance records. Single-factor authentication may not be reasonable, however, for protecting access to highly sensitive information, including health records and information that could be used for identity theft and financial fraud, such as social security numbers (SSNs) and credit card numbers.

While the use of any single factor provides a minimal level of identity authentication assurance, that level is increased greatly by using multiple authentication factors of different types. For example, for "in person" transactions, in the case of a parent or student accessing education records from a school office, the school official might request a photo ID to validate the identity of the person requesting the records. This approach utilizes two factors to validate the identity of the requester—an ownership factor in the form of a valid photo ID and an inherence factor, which is the physical resemblance of the person to the one pictured in the photo ID. Often, this type of visual authentication is not possible for electronic and phone transactions (although video cameras can be used for identifying individuals in some cases, such as for granting physical access to a secure facility).

In addition to using multiple authentication factors, higher levels of assurance can be achieved through the use of authentication factors that are harder to guess or falsify and by implementing stricter mechanisms to protect their secrecy. Stronger factors (e.g., more complex passwords) and better protection from being compromised through malicious activity (e.g., encrypting passwords with a strong algorithm) offer a greater level of confidence in a user's identity authentication. (For more details and best practice suggestions on choosing appropriate authenticating factors, see NIST Special Publication 800-63-1, Electronic Authentication Guideline. For recommendations on strengthening the overall information system security, including tips for generating stronger passwords, see PTAC's Data Security: Top Threats to Data Protection brief.)

How Can an Organization Determine an Adequate Level of Identity Authentication?

FERPA requires that educational agencies and institutions use reasonable methods to identify and authenticate the identity of parents, students, school officials, and other parties before disclosing or permitting access to PII (34 CFR § 99.31[c]). So the question becomes, "How can an educational agency or institution determine the appropriate level of identity authentication assurance?"

To address this question, an organization should conduct a risk assessment to determine the threats to its data and evaluate the likelihood of inappropriate data disclosure based on its specific situation. This assessment should include a review of a potential impact of unauthorized disclosure or, conversely, of inappropriate denial of access to education data (e.g., when an authorized staff member is unable to perform his or her duties due to limited access to data). The analysis of the risks of a potential authentication failure and associated impact should then be used to determine the necessary levels of identity authentication assurance the organization needs to establish. Each organization must individually determine the appropriate level of assurance that would provide, in its specific environment, reasonable means for protecting the privacy of education data it maintains.

The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have released the E-authentication Guidance for Federal Agencies (OMB M04-04), which can be referenced for best practice suggestions on performing risk assessments to identify the threats and potential privacy impacts of unauthorized release of information. The document offers extensive guidance on how to use risk assessment data to determine the required identity authentication assurance level. Figure 1 describes the four levels of assurance defined by NIST.

> Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as (1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
>
> ***Level 1***: *Little or no confidence in the asserted identity's validity.*
>
> ***Level 2***: *Some confidence in the asserted identity's validity.*
>
> ***Level 3***: *High confidence in the asserted identity's validity.*
>
> ***Level 4***: *Very high confidence in the asserted identity's validity.*
>
> ***(OMB M04-04)***

Figure 1 - OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 2003

As a best practice, educational agencies and institutions can leverage this methodology to perform a privacy risk assessment to identify the risks to data privacy and map those risks to assurance levels. Once the risks are understood and the level of identity authentication is well defined, organizations can then choose appropriate technology and authentication tools that provide the required level of identity

authentication. For more in-depth guidance and information on identity authentication tools and technologies associated with various levels of identity assurance, see NIST Special Publication 800-63-1, Electronic Authentication Guideline.

What are Some Reasonable Authentication Practices?

Educational agencies and institutions are required to use "reasonable" authentication methods for all disclosures of PII from education records under FERPA. This includes disclosures of PII made with the written consent of a parent or eligible student, as required under FERPA (34 CFR §99.30), as well as disclosures made without consent under one of the FERPA exceptions listed in 34 CFR §99.31(a). An educational agency or institution must also identify and authenticate the identity of a parent or student before allowing them to inspect and review the student's own records, as permitted under FERPA (34 CFR §99.10). No individual or entity should be allowed unauthenticated access to confidential education records or data at any time.

While the Department does not mandate any specific requirements regarding reasonable methods, some best practice suggestions include:

- conducting privacy risk assessments to determine potential threats to the data;
- selecting authentication levels based on the risk to the data (the higher the risk, the more stringent the authentication);
- developing a process to securely manage any secret authenticating information, or, "authenticators" (e.g., passwords) throughout their creation, use, and disposal;
- enforcing policies to reduce the possibility of authenticator misuse (e.g., encrypting stored passwords, locking out accounts with suspicious activity, etc.); and
- managing user identities through creation, provisioning, use, and disposal (with periodic account recertification, to confirm that a user account has been properly authorized and is still required by the user).

The section below provides more specific recommendations for applying effective authentication procedures; see also NIST Special Publication 800-63-1, Electronic Authentication Guideline and other resources at the end of his document for additional suggestions. As these are best practices, it is up to individual organizations to determine which actions are the most appropriate based on the specific circumstances, including the sensitivity level of the data and the risk of harm associated with unauthorized disclosure.

What Specific Methods for Effective Authentication Can PTAC Recommend?

Depending on the level of assurance required, an educational agency or institution might determine that an application, which allows parents to gain access to "less sensitive" education data, such as

attendance records, by using single-factor authentication (for example, a username and a unique PIN generated upon registration with the system) provides the necessary level of identity authentication. The same organization may have other systems that allow access to "more sensitive" data, such as student financial aid information, health information, or SSNs. In addition to a username and a PIN, these systems might choose to employ additional authentication factors. For example, a school may require parents requesting online access to a student's transcript to answer security questions or confirm their identity by retrieving a one-time password sent to the mobile device they have previously registered with the institution.

It is important to remember that authentication factors like PINs, passwords, and security tokens are only effective if the user is the only party who knows this information or possesses the token. This sometimes makes it difficult to recover a user's ability to access the data from a system if the user has forgotten the password or misplaced his or her token. No agency officials should be able to recover passwords or security tokens for any reason. With that in mind, full, unencrypted passwords in plain text should never be stored within electronic systems. We recommended that you work with your Information Technology (IT) Administrator or Security Officer to ensure that stored passwords are encrypted using a strong cryptographic algorithm. This approach reduces the risk of password data leakage and prevents administrators or school officials from being able to access actual passwords, increasing the assurance level of the system.

In most cases, establishing identity authentication for electronic transactions is more complex than for transactions conducted in person or by phone. Each educational agency or institution must assess its own policies and systems to determine appropriate identity authentication measures based on its own combination of technology, the sensitivity of the data, and applicable data security policies. The risks and privacy impacts may differ significantly by organization depending on the type of data an agency or an institution maintains and on the potential harm caused by the failure to properly secure the data. For example, a school that does not share student records electronically would have a vastly different disclosure risk than a school or an agency that routinely shares education data with partner organizations and offers students online access to their own records. Please keep in mind that an organization may have multiple information systems, which house data of differing sensitivities and privacy impact.

For electronic systems, well designed account recovery mechanisms and cryptographic protection of the authentication process are of great importance and should be incorporated into the system development process. One unwavering fact of electronic data systems is that users will, at some point, lose or forget their account password, PIN, or other authenticating information. It is important that these systems include the ability to safely recover or reset the authenticating information without negatively impacting the integrity of the authentication system. The method might be as simple as an email-based recovery option that asks alternate security questions created during user registration. This type of recovery procedure relies on the knowledge of the security questions, which the user created upon registration, and requires the party being authenticated to have access to the email account utilized for the registration. These two factors together increase the security of the transaction and

allow a user to recover information without delay. (*Additional authentication is not necessary when utilizing a mail or delivery process that authenticates the recipient's identity, because it is structured to deliver the information only to the intended recipient.*)

Identity authentication relies on the secrecy of authentication factors. Consequently, it is advisable that all exchanges of passwords or other authenticating information be sent through encrypted channels using a secure transfer protocol, such as Transport Layer Security. For online systems, organizations should implement basic authentication controls to reduce the ability of an attacker to guess at authentication credentials until the correct combination is achieved (known as "brute force password guessing") by introducing mechanisms to lockout or prevent repetitive failed authentication attempts. The most popular solution is to implement an account lockout mechanism, whereby an account or system is automatically locked after a predefined number of unsuccessful log-on attempts (the account can then be unlocked only by a system administrator or help desk). This approach can help to reduce the threat of brute-force attacks.

Care should be taken when developing and implementing authentication systems within web applications to ensure that the applications are built using secure coding and session management techniques along with thorough validation of user input to prevent attacks like SQL injection, Cross Site Scripting, and Cross Site Request Forgery, among others (see Glossary for definitions of these terms). (For additional data security tips, see PTAC's Data Security: Top Threats to Data Protection brief at http://www.ed.gov/policy/gen/guid/ptac/pdf/issue-brief-threats-to-your-data.pdf).

Additional Resources

Materials below include links to federal regulations and several guidance documents outlining privacy and security issues associated with protecting confidential data through identity authentication. These resources provide best practice recommendations, including frameworks, policies, and procedures for developing and implementing effective identity authentication methods. Please note that some of the guides come from the private sector (marked accordingly) and, as such, they do not necessarily address the legal requirements, including FERPA, that educational agencies and institutions need to meet when storing, disseminating, or releasing education records. The U.S. Department of Education does not endorse private-sector resources; it simply refers them to readers for consideration.

- Department of Justice, *Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* (2000): www.cio.noaa.gov/Policy_Programs/eprocess.pdf
- *FERPA regulations amendment* (2011): www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf
- *FERPA regulations amendment* (2008): www.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf
- Government Technology, *E-Authentication Best Practices for Government* (2011) (private sector resource): www.govtech.com/pcio/articles/E-Authentification-Best-Practices-for-Government.html
- National Institute of Standards and Technology, Complete list of Authentication publications: www.csrc.nist.gov/publications/PubsTC.html#Authentication
- National Institute of Standards and Technology (NIST), NIST SP 800-63-1, *Electronic Authentication Guideline* (2011): www.nist.gov/customcf/get_pdf.cfm?pub_id=910006
- National Institute of Standards and Technology (NIST), NIST SP 800-30, *Guide for Conducting Risk Assessments* (2011) (initial public draft): http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf
- National Institute of Standards and Technology (NIST), NIST SP 800-132, *Recommendation for Password-Based Key Derivation Part 1: Storage Applications* (2010): www.csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
- National Institute of Standards and Technology (NIST), NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* (2008): www.csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf
- National Institute of Standards and Technology (NIST), *Electronic Authentication: Guidance for Selecting Secure Techniques* (2004): www.itl.nist.gov/lab/bulletns/bltnaug04.htm
- National Institute of Standards and Technology, *Standards for Security Categorization of Federal*

Information and Information Systems (2004): www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

- National Institute of Standards and Technology (NIST), NIST SP 800-30, *Risk Management Guide for Information Technology Systems* (2002): http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Office of Management and Budget, Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies* (2003): www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
- Privacy Technical Assistance Center website: www.ed.gov/ptac/
- PTAC, Issue Brief, *Data Security: Top Threats to Data Protection* (2011): www.ed.gov/policy/gen/guid/ptac/pdf/issue-brief-threats-to-your-data.pdf

Glossary

Assurance level is a level of confidence in the process used to validate and establish the identity of a person attempting to access an information system. For more guidance on authentication assurance levels, see E-authentication Guidance for Federal Agencies (OMB M04-04) and NIST SP 800-63-1.

Authentication (single and multifactor) is a mechanism that an electronic system uses to identify and validate the identity of users with the required degree of confidence that the user is who he or she purports to be. Authentication is accomplished through the use of one or more "factors," which correspond to things that the user knows (like a password), something that they possess (like a security token), or something they are (like a fingerprint). Authentication should not be confused with authorization, which is the process of granting individuals access to system resources based on their identity [NIST SP 800-103].

Authenticator is a "secret that creates the binding between credentials and its presenter" [NIST SP 800-103]. Authenticators can take the form of information, such as passwords or PINs; hardware, such as key fobs or smart cards; or some digital form, such as digital signatures and certificates.

Brute-force attack is a type of malicious attack against a system in which the attacker repeatedly attempts to gain access by presenting all possible combinations of access credentials until a match is found. A hacker attempting to gain access to a system by guessing all possible combinations of characters in a password is an example of a brute-force attack.

Cross site request forgery is a type of malicious exploit where an attacker gains access to and executes unauthorized commands on a target web application (e.g., web interface for a network device or web email client) via the browser of an already authenticated user. The attack is accomplished by tricking a validated user who has logged in and has a session cookie stored in the browser into opening an email message or visiting a webpage with imbedded malicious content.

Cross Site Scripting (XSS) is a type of computer security vulnerability that uses malicious script imbedded in an otherwise benign and trusted web application to gather user data. When the script is executed (e.g., when a user clicks on a compromised link in an email message or reads an infected forum post), sensitive user data can be accessed by the attacker.

Cryptographic hash algorithm is a well-defined computational procedure that takes variable inputs (e.g., individual's name or a password in plain text) and produces a fixed-size hash value (also known as message digest), such that any accidental or intentional change of the input (e.g., user mistyping a password) would produce a different hash value.

Education program is defined as any program principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3.

Education records means records directly related to a student and maintained by an educational agency or institution, or by a party acting on behalf of the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Encryption is the process of transforming information using a cryptographic algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key.

Identification is the process that a system uses to recognize a valid user's asserted identity. It is the first step in the authentication and authorization process where the user requesting access is asserting that he or she is a valid user. This differs from the authentication process during which the user provides a proof, or factors that prove that the user really is the person he or she claims to be.

Personally identifiable information (PII) refers to information, such as a student's name or identification number, which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3, for a complete definition of PII specific to education data and for examples of education data elements that can be considered PII.

Security token is a physical (hardware or software) device, which a user possesses that serves to prove that the user requesting access is in fact who he or she claims to be. Examples of tokens include smart cards, key fobs, and USB keys.

Sensitive data are data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) from education records was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010, and NIST SP 800-122, for more information.

Secure file transfer protocol is a broad term referring to network technology used to encrypt authentication information and data files in transit, so that data files can be safely accessed, transferred, and managed.

SQL injection is an attack technique exploiting security vulnerability of a website to gain access to its operations (e.g., to steal, delete, or modify the content of a database). It is often accomplished by inserting malicious SQL statements into user-input field on a web application form.

Transport Layer Security (TLS) is a cryptographic network protocol that provides authentication, confidentiality, and data integrity between two communicating applications. TLS is used as a mechanism to protect sensitive data during electronic dissemination across the Internet.