



---

## **Accessibility and Accommodations Manual**

---

Prepared by the  
Administration,  
Accessibility, and  
Accommodations  
Task Management  
Team

---

November, 2014

---

English Language Proficiency Assessment for the 21<sup>st</sup> Century

Table of Contents

**Introduction**..... 3  
Intended Audience and Recommended Use..... XX  
ELPA21 Assessment Features.....  
Accessibility Features and Accommodations Conceptual Model.....  
Recognizing Accessibility Needs in All Students.....  
Structure of This Document.....

**Section I: ELPA21 Universal Features**.....  
What Are Universal Features?.....  
Embedded Universal Features.....  
Non-embedded Universal Features.....

**Section II: ELPA21 Designated Features**.....  
What Are Designated Features?.....  
Who Makes Decisions About Designated Features? .....  
Embedded Designated Features.....  
Non-embedded Designated Features.....

**Section III: ELPA21 Accommodations**.....  
What Are Accommodations?.....  
Who Makes Decisions About Accommodations?.....  
Embedded Accommodations.....  
Non-embedded Accommodations.....

**Resources**.....

**Appendices**.....  
Appendix A: Field Test Universal Features, Designated Features, and  
Accommodations.....  
Appendix B: Field Test Assistive Technology.....

## Introduction

The English Language Proficiency Assessment for the 21<sup>st</sup> Century (ELPA21) Consortium is committed to providing assessments that best measure rigorous English Language Proficiency Standards ([hyperlink](#)) that correspond to college- and career-ready content standards in mathematics, English language arts, and science. The assessments are designed to provide information for instruction and to facilitate the acquisition of academic English proficiency needed for college and career success after high school. ELPA21 is designing its next-generation assessments with all English language learners (ELLs) – including those who have disabilities – in mind, recognizing that the validity of assessment results depends on each and every student having appropriate access to the assessment. This *Accessibility and Accommodations Manual* was developed for the ELPA21 member states to guide the selection and administration of appropriate universal features, designated features, and accommodations for individual students to produce valid assessment results.

The universal features, designated features, and accommodations for the ELPA21 assessments may be different from those available for states' previous assessments of English language proficiency (ELP). To ensure secure and valid administration of the ELPA21 assessments, ELPA21 member states may only make available to students those universal features, designated features, and accommodations, as appropriate, that are included in this *Manual*.

Although some of the accessibility features and accommodations are not available on the ELPA21 2015 field test, all of them will be available on the operational ELPA21. Appendix A provides the list of universal features, designated features, and accommodations that are available on the field test. If additional or alternative universal features, designated features, and accommodations are identified in the future based on empirical and research recommendations, this *Manual* will be updated to reflect these changes.

### Intended Audience and Recommended Use

The ELPA21 *Accessibility and Accommodations Manual* is intended for district and school-level personnel, as well as decision-making teams, including Individualized Education Program (IEP) teams, as they prepare for and implement the ELPA21 assessments. The *Manual* provides information for classroom teachers, English development educators, special education teachers, and related services personnel to use in selecting and administering universal features, designated features, and accommodations for those students who need them. The *Manual* is also intended for assessment staff and administrators who oversee the decisions that are made in instruction and assessment.

The ELPA21 *Accessibility and Accommodations Manual* applies to all students who take the ELPA21 assessments. It emphasizes an individualized approach to the implementation of assessment practices for those students who have diverse needs and participate in large-scale ELP assessments. This *Manual* focuses on ELPA21's universal features, designated features, and accommodations. At the same time, it supports important instructional decisions about accessibility and accommodations for students who participate in the ELPA21 assessments. It recognizes the critical connection between accessibility and accommodations in instruction and accessibility and accommodations during assessment.

## ELPA21 Assessment Features

The ELPA21 Consortium supports the development of an assessment system for ELLs that reflects the research and progress made in the development of ELP assessments. ELPA21's approach to assessment is rooted in the belief that ELLs are a diverse group; all ELLs are capable of making progress toward English language proficiency; and ELLs must acquire discipline-specific language practices that enable them to produce, interpret, and effectively collaborate on content-related grade-appropriate tasks.

The ELPA21 assessment system, which includes a screener and a summative assessment of reading, writing, speaking, and listening, supports individual ELLs and their schools and districts by:

- determining initial identification of ELLs through the screener;
- monitoring ELLs' yearly progress in the attainment of English for academic purposes;
- measuring districts' success in meeting Title III accountability benchmarks; and
- informing decisions about exiting students from ELD services provided under Title III.

For more information on ELPA21, visit [www.elpa21.org](http://www.elpa21.org).

## Accessibility Features and Accommodations Conceptual Model

ELPA21 states worked together through the Administration, Accessibility, and Accommodations Task Management Team to develop the ELPA21 conceptual model for accessibility and accommodations, and to determine which universal features, designated features, and accommodations are needed for equitable access and valid assessment results. The conceptual model, shown in Figure 1, highlights: (a) universal features (supports available to all students), (b) designated features (supports available for individual students that must be assigned to students in advance of testing), and (c) accommodations (supports available to individual students with Individualized Education Programs – IEPs – or 504 plans; accommodations must be assigned to students in advance of testing). In addition, it shows some of the administrative considerations that support the participation of students in the ELPA21 assessments. These administrative considerations are provided in detail in the *ELPA21 Administration Manual* ([hyperlink](#)). **Note: To ensure valid and secure administration of the ELPA21 assessments, only those universal features, designated features, and accommodations explicitly identified in this *Manual* may be used during test administration.**

Figure 1 also lists the embedded supports (provided digitally as components of the test administration system) and non-embedded supports (provided locally with human assistance). The identified universal features, designated features, and accommodations all yield valid scores that count as participation in the ELP assessments when used in a manner consistent with the *Manual*.

### Figure 1. Conceptual Model of ELPA21 Accessibility Features and Accommodations

## Universal Features (available to all students)

**Embedded:** amplification, answer choice eliminator, audio support, digital notepad, expandable passages, highlighter, mark for review, text-to-speech (for writing), writing tools, zoom (item-level)

**Non-embedded:** familiar examiner, read aloud (for writing), scratch paper

## Designated Features (identified in advance)

**Embedded:** color contrast, color overlay, line reader, masking, native language translation of directions (includes ASL), spellcheck, turn off universal features

**Non-embedded:** magnification device, noise buffer, print on request, student reads test aloud

## Accommodations (available with an IEP or 504 plan)

**Embedded:** extended time, replaying items (for listening)

**Non-embedded:** answer orally, assistive technology, braille, large print test booklet, scribe

**Administrative Considerations**, e.g., breaks, setting adjustments (adaptive furniture, carrel, Individual, lighting/acoustics, minimal distractions, seating location, small group), re-read directions, testing at time beneficial to student. See the *Administration Manual* ([hyperlink](#)) for the complete list and additional information on administrative considerations.

This conceptual model was developed to ensure that the ELPA21 assessments meet each student's unique accessibility needs. It also recognizes that some students may have characteristics and access needs that require the use of accommodations during instruction and when they participate in the ELPA21 assessments.

This *Accessibility and Accommodations Manual* presents the universal features, designated features, and accommodations adopted by the ELPA21 states to ensure valid assessment results for all students participating in the ELPA21 assessments. See Appendix A for the features and accommodations available during the ELPA21 field test.

## Recognizing Accessibility Needs in All Students

Both Titles I and III of the Elementary and Secondary Education Act (ESEA) require states and

local education agencies to annually assess the English language proficiency of all ELLs in the state enrolled in public schools in grades kindergarten through twelve in the domains of Speaking, Listening, Reading, and Writing (Sections 1111(b)(7) and 1123(b)(3)(D) of the ESEA). The only exception is for students with the most significant cognitive disabilities who meet the criteria for an alternate ELP assessment that is based on alternate achievement standards.

The ELPA21 assessments are designed for all ELLs, including those who have disabilities (except those participating in the alternate ELP assessment). To better understand student populations served by ELPA21 assessments, educators should consider the following two definitions:

1) **English language learners (ELLs)** are students who meet the following federal definition: the term “limited English proficient,” when used with respect to an individual, means an individual –

(A) who is aged 3 through 21;

(B) who is enrolled or preparing to enroll in an elementary school or secondary school;

(C) (i) who was not born in the United States or whose native language is a language other than English;

(ii) (I) who is a Native American or Alaska Native, or a native resident of the outlying areas; and

(II) who comes from an environment where a language other than English has had a significant impact on the individual's level of English language proficiency;

or

(iii) who is migratory, whose native language is a language other than English, and who comes from an environment where a language other than English is dominant; and

(D) whose difficulties in speaking, reading, writing, or understanding the English language may be sufficient to deny the individual —

(i) the ability to meet the State's proficient level of achievement on State assessments described in Section 1111(b)(3);

(ii) the ability to successfully achieve in classrooms where the language of instruction is English; or

(iii) the opportunity to participate fully in society.

2) **English language learners (ELLs) with disabilities** are ELLs who have a 504 accommodation plan or an Individualized Education Program (IEP). Those with an IEP may be identified as having one or more categories of disability (autism, deaf blind, developmental delay, emotional disturbance, hearing impairment and deafness, intellectual disability, multiple disabilities, other health impairment, orthopedic impairment, specific learning disability, speech language impairment, traumatic brain injury, and visual impairment and blindness).

According to guidance released by the U.S. Department of Education (July 18, 2014), all ELLs with disabilities are required to participate in annual state ELP assessments. If needed, students must be provided individual appropriate accommodations in accordance with a student's IEP team. The IEP team for an ELL with a disability should include at least one person in second language acquisition. The IEP team is responsible for deciding how an ELL with a disability should participate in ELP assessments – in regular ELP assessments without accommodations, in regular ELP assessments with accommodations that do not invalidate the test constructs, or in alternate ELP assessments.

To ensure that ELLs with disabilities are receiving appropriate accessibility features and accommodations, IEP team members should consider the degree of each student’s language- and disability-related needs. Accessibility and accommodation decisions should be individualized based on the particular language- and disability-related challenges faced by ELLs with disabilities. Students with high English language needs and low disability-related needs will require more language-based supports while their counterparts with high disability-related needs and low English language needs will require more supports that remove disability-related barriers. At the same time, students with high English language needs and high disability-related needs will benefit from more intensive language- and disability-related supports while students with low English language needs and low disability-related needs will require fewer supports that alleviate linguistic and disability-related assessment challenges.

## Structure of This Document

This *Accessibility and Accommodations Manual* consists of the following parts:

- **Introduction:** This section addresses the intended audience and recommended use of the document, introduces the ELPA21 assessments as well as the conceptual model that underlies the accessibility and accommodations approaches, and describes participating students’ characteristics and some considerations for administering the ELPA21 assessments.
- **Section I:** This section features the ELPA21 universal features.
- **Section II:** This section features the ELPA21 designated features.
- **Section III:** This section features the ELPA21 accommodations.
- **Resources:** This section lists some resources that provide additional information on accessibility features and accommodations.
- **Appendices:** This section includes appendices with additional information on ELPA21 assessments.

## Section I: ELPA21 Universal Features

### What Are Universal Features?

**Universal features** are accessibility tools of the ELPA21 assessment that are either provided digitally through the assessment technology (embedded) or non-digitally at the local level (non-embedded). Universal features are available to all students based on student preference and selection.

### Embedded Universal Features

The ELPA21 digitally-delivered assessments include a wide range of embedded universal features. These features are available to all students as part of the technology platform.

Table 1 lists the embedded universal features available to all students for digitally-delivered ELPA21 assessments. It also includes a description of each feature. Although these features are generally available to all students, educators may determine that one or more might be distracting for a particular student, and thus might indicate that the feature should be turned off for the administration of the assessment to the student (see Section II – Designated Features).

**Table 1. Embedded Universal Features Available to All Students**

Universal Feature	Description
Amplification	The student raises or lowers the volume control, as needed, using headphones.
Answer choice eliminator	The student uses this feature to eliminate those answer choices that do not appear correct to the student.
Audio support	The student uses this feature to hear pre-recorded audio of most tasks. With the exception of the text in drag-and-drop text and the text in a word bank audio support is available for the following: Speaking – all tasks have audio support for all components; Listening – all tasks have audio support for all components; Writing – all tasks have audio support for all components except for inline editing tasks; and Reading – no audio support is available except for read-along tasks and for all K tasks and items.
Digital notepad	The student uses this feature as virtual scratch paper to make notes, write computations, or record responses. The digital notepad is item-specific and is available through the end of each test domain. Notes are not saved when the student moves on to a different test domain or after a break of more than 20 minutes.
Expandable passages	The student is able to expand each passage so that it takes up a larger portion of the screen as the student reads. The student can then retract the passage to its original size.
Highlighter	The student uses this digital feature for marking desired text, items, or response options with the color yellow. Highlighted text remains available throughout the test.
Mark for review	The student is able to flag items for future review during the assessment.

	Markings are not saved when the student moves on to another test domain, or after pausing the test for more than 20 minutes.
Text-to-speech (for writing)	The student is able to have the prompt read aloud for any writing item read via the text-to-speech feature.
Writing tools	The student uses writing tools to format and edit written responses, including cut and paste, copy, underline, italicize, bold, undo/redo, and insert bullets.
Zoom (item-level)	The student can enlarge the size of text and graphics on a given screen. This feature allows students to view material in magnified form on an as-needed basis. The student may enlarge test content at least fourfold. The system allows magnifying features to work in conjunction with other accessibility features and accommodations provided.

### Non-embedded Universal Features

Some universal features may need to be provided locally outside of the computer administration system. These features are shown in Table 2. They can be made available to any student.

**Table 2. Non-embedded Universal Features Available to All Students**

Universal Feature	Description
Familiar examiner	The student's assessment is administered by a test administrator who has previously worked with the student in assessment or instruction settings. This universal feature should be used only if there is a strong rationale for having a familiar examiner. If a familiar examiner does administer the assessment, that person must have completed all training and sign a document indicating compliance with test security and ethical practices.
Read aloud (for writing)	The student has the prompt for any writing item read by a human reader who has completed all training and signed a document indicating compliance with test security and ethical practices.
Scratch paper	The student uses scratch paper to make notes, write computations, or record responses. All scratch paper must be collected and securely destroyed at the end of each test domain to maintain test security. The student can use an assistive technology device for scratch paper as long as the device is approved by the ELPA21 consortium. Test administrators have to ensure that all the notes taken on an assistive technology device are deleted after the test.

## Section II: ELPA21 Designated Features

### What Are Designated Features?

**Designated features** for the ELPA21 assessments are those features (embedded and non-embedded) that are available for use by any student for whom the need has been indicated by an educator (or team of educators with parent/guardian and student). Designated features must be assigned to a student in advance of test administration by trained educators or teams using a consistent process.

### Who Makes Decisions About Designated Features?

Decisions about designated features should be made by educators (or teams of educators, with parent/guardian and student) who are familiar with the student’s characteristics and needs. Decisions should reflect those supports that the student uses during instruction and for other assessments. Student input to the decision, particularly for older students, is recommended.

ELPA21 professional development materials provide suggested processes that may be used if a district or school does not have an existing process in place for adults and others to make decisions about designated features. The Personal Needs Profile (PNP), created and provided by ELPA21, is used to document which designated features a student needs and that will be made available to that student during the assessment. All embedded designated features must be activated via the PNP prior to testing.

### Embedded Designated Features

Table 3 shows the ELPA21 embedded designated features. It includes a description of each feature along with recommendations for when a student might benefit from using the feature.

**Table 3. Embedded Designated Features Identified in Advance**

Designated Feature	Description	Recommendations for Use
Color contrast	The student is able to adjust the text color and screen background color based on the student’s need. The color contrast options, in addition to the default black text on white background, include: 1) black text on cream background; 2) black text on light blue background; 3) black text on light pink background; 4) yellow text on blue background; and 5) white text on black background.	Students with attention difficulties may need this feature for viewing test content. It also may be needed by some students with visual impairments or other print disabilities (including learning disabilities). Choice of colors should be informed by evidence that specific text and background color combinations meet the student’s needs.
Color overlay	The student is able to overlay a	This designated feature only works with

	semitransparent color onto test content.	black text on white background.
Line reader	The student is able to use this feature as a guide when reading text.	Students with attention difficulties or reading disabilities may need assistance with tracking where they are reading.
Masking	The student is able to block off content that is not of immediate need or that may be distracting. Masking allows students to hide and reveal individual answer options, as well as all navigational buttons and menus. The student is able to focus his/her attention on a specific part of a test item by masking.	Students with attention difficulties may need to mask content not of immediate need or that may be distracting during the assessment. This feature also may be needed by students with print disabilities (including learning disabilities) or visual impairments.
Native language translation of directions (includes ASL)	Translation of general (not item-specific) test directions (not prompts or questions) is a language support available prior to the student being presented with the actual test items. The student can see test directions in another language. <b>The following are the languages in which directions are provided: ASL,</b> [to be added as decisions are made]	Students who have limited English language skills can use the translated directions feature.
Spellcheck <b>(needs some decision making)</b>	This feature allows the student to check the spelling of words in student-generated responses. Spellcheck only gives an indication that a word is misspelled; it does not provide the correct spelling.	[To be added after decisions are made]
Turn off universal features	This feature allows disabling any universal feature that might interfere with student performance, or be distracting to the student.	Students who are easily distracted (whether or not designated as having attention difficulties or disabilities) may be overwhelmed by some of the universal features. Having evidence of which specific features may be distracting is important for determining which features to turn off.

## Non-embedded Designated Features

Some designated features may need to be provided outside of the digital-delivery system. These features are shown in Table 4. They are to be provided locally for those students unable to use the embedded designated features.

**Table 4. Non-embedded Designated Features Identified in Advance**

<b>Designated Feature</b>	<b>Description</b>	<b>Recommendations for Use</b>
Magnification device	The student adjusts the size of specific areas of the screen (e.g., text, formulas, tables, and graphics) with an assistive technology device. Magnification allows increasing the size to a level not provided for by the zoom universal feature.	Students with visual impairments may need to increase the size of text and other item features beyond the 4X zoom universal feature provided by the test platform.
Noise buffer	The student uses noise buffers to minimize distraction or filter external noise during testing. Any noise buffer must be compatible with the requirements of the test (e.g., allow the student to hear listening items).	Students who are distracted by external noises within the testing environment may need noise buffers (e.g., headphones, mufflers).
Print on request	The student uses paper copies of entire test items.	Students may not be able to interact with items online (due to visual impairments, lack of familiarity with the computer-based format, or other cultural reasons), and as a result may need a paper copy of test items. The use of this accommodation may result in the student needing additional time to complete the assessment. A very small percentage of students should need this designated feature.
Student reads test aloud	The student reads the test content aloud. This feature must be administered in a one-on-one test setting.	Students who are beginning readers may need to hear themselves read in order to comprehend text.

## Section III: ELPA21 Accommodations

### What Are Accommodations?

**Accommodations** are changes in procedures or materials (embedded and non-embedded) that increase equitable access during the ELPA21 assessments and generate valid assessment results for students who need them. Accommodations are for students for whom there is documentation of need on an Individualized Education Program (IEP) or 504 accommodation plan so that these students show what they know and can do on the ELPA21 assessments.<sup>2</sup>

### Who Makes Decisions About Accommodations?

IEP teams and educators for 504 plans make decisions about accommodations. These decision makers provide evidence of the need for accommodations and ensure that they are noted on the IEP or 504 plan. Decision makers are responsible for entering information on accommodations for ELPA21 from the IEP/504 plan into the PNP so that all embedded accommodations can be activated prior to testing. This can be accomplished by identifying one person (for example, a team member or a test coordinator) enter information into the PNP prior to testing.

### Embedded Accommodations

Table 5 lists the embedded accommodations available for the ELPA21 assessments. The table includes a description of each accommodation along with recommendations for when the accommodation might be needed and how it can be used.

**Table 5. Embedded Accommodations Available with an IEP or 504 Plan**

<b>Accommodation</b>	<b>Description</b>	<b>Recommendations for Use</b>
Extended time	The student uses extended time to complete testing. A maximum of up to one school day is allowed to complete one test domain during the prescribed testing window. Students who use this accommodation must be given a quiet location in which to complete the test.	Students require additional time because of testing fatigue, memory load issues, or medication requirements.
Replaying test items (for listening)	The student replays a listening item as many times as needed (beyond the default of two plays).	Students with hearing impairments or attention issues may require additional listening opportunities.

---

<sup>2</sup> The exception to the IEP or 504 requirement is for students who have had a physical injury (e.g., broken hand or arm) that impairs their ability to use a computer. These students may use the speech-to-text or the scribe accommodations (if they have had sufficient experience with the use of these), as noted in this section.

## Non-embedded Accommodations

Table 6 shows the ELPA21 non-embedded accommodations. The table includes a description of each accommodation, along with recommendations for when the accommodation might be needed and how it can be used.

**Table 6. Non-embedded Accommodations Available with an IEP or 504 Plan**

Accommodation	Description	Recommendations for Use
Answer orally	The student dictates responses either verbally, using a speech-to-text device, augmentative/assistive communication device (e.g., picture/word board), or by signing, gesturing, pointing, or eye-gazing. Grammar checker, Internet access, and stored files functionalities must be turned off. Word prediction must also be turned off for students who do not receive this accommodation.	Students who are unable to use a keyboard or mouse may need to respond orally to a human scribe or transcriber.
Assistive technology	The student is able to use assistive technology, which includes such supports as typing on customized keyboards, assistance with using a mouse, mouth or head stick or other pointing devices, sticky keys, touch screen, and trackball, speech-to-text conversion, or voice recognition. The starting list of assistive technology devices available on the ELPA21 field test is included in Appendix B.	Students who have difficulty manipulating a mouse or standard keyboard may need an alternative device.
Braille	A raised-dot code that individuals read with the fingertips. Graphic material (e.g., maps, charts, graphs, diagrams, and illustrations) is presented in a raised format (paper or thermoform). Both contracted and uncontracted braille (English Braille, American Edition) are available; Unified English Braille will be adopted for future assessments.	Students who are blind or have low vision may read text via braille. Tactile overlays and graphics also may be used to assist the student in accessing content through touch. The use of this accommodation may result in the student needing additional overall time to complete the assessment.
Large print test booklet	The student uses a large print form of the test is provided to the student with a visual impairment. The font size for the large print form is 18 point on paper sized 11 x 17.	Students with visual impairments may not be able to use zoom or magnifying devices to access the test may need a large print version of the form.
Scribe	The student dictates her/his responses to a human who records verbatim what the student dictates. A scribe is a skilled person who has	Students who have documented significant motor or processing difficulties, or who have had a recent injury (such as a broken

	<p>been trained to write down what a student dictates by an assistive communication device, pointing, sign language, or speech. It is important that the student is able to develop planning notes via the human scribe, and to view what was produced while composing via dictation to the scribe.</p>	<p>hand or arm) that makes it difficult to produce responses may need to dictate their responses to a human, who then records the students' responses verbatim. The use of this accommodation may result in the student needing additional time to complete the assessment. For many of these students, dictating to a human scribe is the only way to demonstrate their composition skills.</p>
--	---	--

## Resources

Christensen, L., Shyyan, V., Schuster, T., Mahaley, P., & Saez, S. (2012). Accommodations manual: How to select, administer, and evaluate use of accommodations for instruction and assessment of English language learners. Minneapolis, MN: University of Minnesota, National Center on Educational Outcomes. Available at:

<http://www.cehd.umn.edu/NCEO/OnlinePubs/ELLSManual090612.pdf>

National Center on Educational Outcomes. (2009). Accommodations bibliography. Minneapolis, MN: University of Minnesota, National Center on Educational Outcomes. Available at:

<https://apps.cehd.umn.edu/nceo/accommodations/>

Partnership for Assessment of Readiness for College and Careers. (2014). PARCC accessibility features and accommodations manual. Available at:

<http://www.parcconline.org/parcc-accessibility-features-and-accommodations-manual>

Shyyan, V., Christensen, L., Touchette, B., Lightborne, L., Gholson, M., & Burton, K. (2013). Accommodations manual: How to select, administer, and evaluate use of accommodations for instruction and assessment of English language learners with disabilities. Minneapolis, MN: University of Minnesota, National Center on Educational Outcomes. Available at:

<http://www.cehd.umn.edu/NCEO/OnlinePubs/ELLSWDAccommodationsManual.pdf>

Smarter Balanced Assessment Consortium. (2014). Usability, accessibility, and accommodations guidelines. Available at: [http://www.smarterbalanced.org/wordpress/wp-content/uploads/2014/08/SmarterBalanced\\_Guidelines.pdf](http://www.smarterbalanced.org/wordpress/wp-content/uploads/2014/08/SmarterBalanced_Guidelines.pdf)

## Appendices

### Appendix A: Field Test Universal Features, Designated Features, and Accommodations

**Table A. Field Test Embedded Universal Features Available to All Students**

Universal Feature	Description
Amplification	The student raises or lowers the volume control, as needed, using headphones.
Answer choice eliminator	The student uses this feature to eliminate those answer choices that do not appear correct to the student.
Audio support	The student uses this feature to hear pre-recorded audio of most tasks. With the exception of the text in drag-and-drop text and the text in a word bank audio support is available for the following: Speaking – all tasks have audio support for all components; Listening – all tasks have audio support for all components; Writing – all tasks have audio support for all components except for inline editing tasks; and Reading – no audio support is available except for read-along tasks and for all K tasks and items.
Digital notepad	The student uses this feature as virtual scratch paper to make notes, write computations, or record responses. The digital notepad is item-specific and is available through the end of each test domain. Notes are not saved when the student moves on to a different test domain or after a break of more than 20 minutes.
Expandable passages	The student is able to expand each passage so that it takes up a larger portion of the screen as the student reads. The student can then retract the passage to its original size.
Highlighter	The student uses this digital feature for marking desired text, items, or response options with the color yellow. Highlighted text remains available throughout the test.
Mark for review	The student is able to flag items for future review during the assessment. Markings are not saved when the student moves on to another test domain, or after pausing the test for more than 20 minutes.
Text-to-speech (for writing)	The student is able to have the prompt read aloud for any writing item read via the text-to-speech feature.
Writing tools	The student uses writing tools to format and edit written responses, including cut and paste, copy, underline, italicize, bold, undo/redo, and insert bullets.
Zoom (item-level)	The student can enlarge the size of text and graphics on a given screen. This feature allows students to view material in magnified form on an as-needed basis. The student may enlarge test content at least fourfold. The system allows magnifying features to work in conjunction with other accessibility features and accommodations provided.

**Table B. Field Test Non-embedded Universal Features Available to All Students**

<b>Universal Feature</b>	<b>Description</b>
Familiar examiner	The student's assessment is administered by a test administrator who has previously worked with the student in assessment or instruction settings. This universal feature should be used only if there is a strong rationale for having a familiar examiner. If a familiar examiner does administer the assessment, that person must have completed all training and sign a document indicating compliance with test security and ethical practices.
Read aloud (for writing)	The student has the prompt for any writing item read by a human reader who has completed all training and signed a document indicating compliance with test security and ethical practices.
Scratch paper	The student uses scratch paper to make notes, write computations, or record responses. All scratch paper must be collected and securely destroyed at the end of each test domain to maintain test security. The student can use an assistive technology device for scratch paper as long as the device is approved by the ELPA21 consortium. Test administrators have to ensure that all the notes taken on an assistive technology device are deleted after the test.

**Table C. Field Test Embedded Designated Features Identified in Advance**

<b>Designated Feature</b>	<b>Description</b>	<b>Recommendations for Use</b>
Color contrast	The student is able to adjust the text color and screen background color based on the student's need. The color contrast options, in addition to the default black text on white background, include: 1) black text on cream background; 2) black text on light blue background; 3) black text on light pink background; 4) yellow text on blue background; and 5) white text on black background.	Students with attention difficulties may need this feature for viewing test content. It also may be needed by some students with visual impairments or other print disabilities (including learning disabilities). Choice of colors should be informed by evidence that specific text and background color combinations meet the student's needs.
Color overlay	The student is able to overlay a semitransparent color onto test content.	This designated feature only works with black text on white background.
Line reader	The student is able to use this feature as a guide when reading text.	Students with attention difficulties or reading disabilities may need assistance with tracking where they are reading.
Masking	The student is able to block off content that is not of immediate need or that may be distracting. Masking allows students to hide and reveal individual answer	Students with attention difficulties may need to mask content not of immediate need or that may be distracting during the assessment. This feature also may be needed by students with print

	options, as well as all navigational buttons and menus. The student is able to focus his/her attention on a specific part of a test item by masking.	disabilities (including learning disabilities) or visual impairments.
Native language translation of directions (includes ASL)	Translation of test directions (not prompts or questions) is a language support available prior to the student being presented with the actual test items. The student can see test directions in another language. The following are the languages in which directions are provided: ASL, [to be added as decisions are made]	Students who have limited English language skills can use the translated directions feature.
Turn off universal features	This feature allows disabling any universal feature that might interfere with student performance, or be distracting to the student.	Students who are easily distracted (whether or not designated as having attention difficulties or disabilities) may be overwhelmed by some of the universal features. Having evidence of which specific features may be distracting is important for determining which features to turn off.

**Table D. Field Test Non-embedded Designated Features Identified in Advance**

<b>Designated Feature</b>	<b>Description</b>	<b>Recommendations for Use</b>
Magnification device	The student adjusts the size of specific areas of the screen (e.g., text, formulas, tables, and graphics) with an assistive technology device. Magnification allows increasing the size to a level not provided for by the zoom universal feature.	Students with visual impairments may need to increase the size of text and other item features beyond the 4X zoom universal feature provided by the test platform.
Noise buffer	The student uses noise buffers to minimize distraction or filter external noise during testing. Any noise buffer must be compatible with the requirements of the test (e.g., allow the student to hear listening items).	Students who are distracted by external noises within the testing environment may need noise buffers (e.g., headphones, mufflers).
Student reads test aloud	The student reads the test content aloud. This feature must be administered in a one-on-one test setting.	Students who are beginning readers may need to hear themselves read in order to comprehend text.

**Table E. Field Test Embedded Accommodations Available with an IEP or 504 Plan**

Accommodation	Description	Recommendations for Use
Extended time	The student uses extended time to complete testing. A maximum of up to one school day is allowed to complete one test domain during the prescribed testing window. Students who use this accommodation must be given a quiet location in which to complete the test.	Students require additional time because of testing fatigue, memory load issues, or medication requirements.
Replaying test items (for listening)	The student replays a listening item as many times as needed (beyond the default of two plays).	Students with hearing impairments or attention issues may require additional listening opportunities.

**Table F. Field Test Non-embedded Accommodations Available with an IEP or 504 Plan**

Accommodation	Description	Recommendations for Use
Answer orally	The student dictates responses either verbally, using a speech-to-text device, augmentative/assistive communication device (e.g., picture/word board), or by signing, gesturing, pointing, or eye-gazing. Grammar checker, Internet access, and stored files functionalities must be turned off. Word prediction must also be turned off for students who do not receive this accommodation.	Students who are unable to use a keyboard or mouse may need to respond orally to a human scribe or transcriber.
Assistive technology	The student is able to use assistive technology, which includes such supports as typing on customized keyboards, assistance with using a mouse, mouth or head stick or other pointing devices, sticky keys, touch screen, and trackball, speech-to-text conversion, or voice recognition.	Students who have difficulty manipulating a mouse or standard keyboard may need an alternative device.
Braille	A raised-dot code that individuals read with the fingertips. Graphic material (e.g., maps, charts, graphs, diagrams, and illustrations) is presented in a raised format (paper or thermoform). Both contracted and uncontracted braille (English Braille, American Edition) are available; Unified English Braille will be adopted for future assessments.	Students who are blind or have low vision may read text via braille. Tactile overlays and graphics also may be used to assist the student in accessing content through touch. The use of this accommodation may result in the student needing additional overall time to complete the assessment.
Scribe	The student dictates her/his responses to a human who records verbatim what the student dictates. A scribe is a skilled person who has	Students who have documented significant motor or processing difficulties, or who have had a recent injury (such as a broken

	<p>been trained to write down what a student dictates by an assistive communication device, pointing, sign language, or speech. It is important that the student is able to develop planning notes via the human scribe, and to view what was produced while composing via dictation to the scribe.</p>	<p>hand or arm) that makes it difficult to produce responses may need to dictate their responses to a human, who then records the students' responses verbatim. The use of this accommodation may result in the student needing additional time to complete the assessment. For many of these students, dictating to a human scribe is the only way to demonstrate their composition skills.</p>
--	---	--

## **Appendix B: Field Test Assistive Technology**

BigKeys Keyboard

BIGtrack Trackball

Headmouse Extreme (Windows only)

Intellikeys Keyboard

KinderBoard Keyboard

Roller II Joystick

Roller Plus Joystick

Switch Interface Pro (Windows only)



**ELPA21 Field Test and Platform and System Trial**  
**Headset Specifications**

The table below outlines features for headsets and Questar’s rationale in recommending those features. Please note that Questar does not endorse specific brands or devices.

<b>Recommended Features</b>	<b>Reason for Recommendation</b>	<b>Alternatives not Recommended</b>
<b>Device:</b> <i>Headset with attached microphone</i>	Allows for recording and playback using the same device.	Separate headphones and microphone increase the need to ensure proper connection and setup on the computer and complicate the testing site set-up.
<b>Headset Design:</b> <i>Over Ear Headphones</i>	Comfortable to be worn for a longer period of time by students of different ages. Weight and size of headphones can be selected based on students’ age. Portable headphones are smaller and lighter and hence may be suitable for younger students.	In ear headphones (ear buds) – for the general population - that are placed directly in the ear canal are more difficult to clean between uses. They may not be suitable for younger students. Ear bud microphones are attached to the cord, making capturing the students’ voice more problematic.
<b>Play Back Mode:</b> <i>Stereo</i>	The sound files of the assessment are recorded and played back in stereo.	Mono headsets
<b>Noise Cancellation Feature:</b> <i>None Needed</i>	Noise cancellation often does not cancel out the sound of human voices.	Many headsets with a noise cancellation feature require a power source, this adds cost and complicates the testing set-up.
<b>Type of Connector Plug:</b> <i>one 3.5 mm Plug, two 3.5 mm Plugs or USB connector</i>	Headsets must be compatible with the computer used for testing. Headsets with two 3.5 mm plugs can be converted with a “Y” adaptor to a single plug and be used with tablets. USB-connected headsets require driver installation and may need to be enabled as playback/recording device.	NOTE: USB-connected headsets for iPads and Android tablets are not available/supported.  Bluetooth is not recommended.
<b>Special Considerations</b>	Alternative size headsets may need to be considered for smaller children, although not required. Ear buds with a microphone may be considered for students who wear head scarves or wraps, etc.	

\*Questar recommends avoiding microphones with windscreens (e.g. foam covers), unless they are removable, to assist with cleaning between uses.

\*\*Please Note: These specifications are for the ELPA21 Field Test only. ELPA21 does not yet have an operational vendor.

\*THE CONTENTS OF THIS DOCUMENT WERE DEVELOPED UNDER A GRANT FROM THE U.S. DEPARTMENT OF EDUCATION. HOWEVER, THESE CONTENTS DO NOT NECESSARILY REPRESENT THE POLICY OF THE U.S. DEPARTMENT OF EDUCATION AND YOU SHOULD NOT ASSUME ENDORSEMENT BY THE FEDERAL GOVERNMENT.\*



**ELPA21 Field Test and Platform and System Trial**  
**Hardware Specifications**

Application	Operating System	OS Version	Processor	System Memory	Hard Disk Space	Screen Size Resolution	LAN Network	In
<b>ELPA21 Field Test Uses a Secure Browser</b>	Windows	XP/Vista/7/8/2003/2008 (latest service pack) <b>(NOTE: Windows 8 RT is not supported)</b>	Intel Pentium 4 1.0 GHz equivalent or higher CPU Recommended Intel Core 2 Duo 1.6 Ghz equivalent or higher performing CPU or higher performing CPU	Minimum 256MB Free Ram Recommended 512 MB Free Ram	Minimum 1 GB Free Storage Space	Minimum 10" class screen size (10" class is 9.5 to 10.5 inches) Minimum 1024 X 768 screen resolution Recommended 12" or larger screen size	Minimum 100 Mbps LAN/802.11g Wireless 54 Mbps or greater Minimum available LAN bandwidth at each workstation: 1 Mbps Recommended 1 Gbps LAN/802.11n Wireless 150 Mbps or higher Recommended available LAN bandwidth at each workstation 2 Mbps	Minimum kps (Minimum caching 3 Recommended)  A secure used.  If more testing si proctor o required.
	Mac	10.6/10.7/10.8/10.9	Intel Core 2 Duo 1.6 GHz equivalent or higher performing CPU	Minimum 256MB Free Ram Recommended 512 MB Free Ram	Minimum 1 GB Free Storage Space	Minimum 10" class screen size (10" class is 9.5 to 10.5 inches) Minimum 1024 X 768 screen resolution Recommended 12" or larger screen size	Minimum 100 Mbps LAN/802.11g Wireless 54 Mbps or greater Minimum available LAN bandwidth at each workstation: 1 Mbps Recommended 1 Gbps LAN/802.11n Wireless 150 Mbps or higher Recommended available LAN bandwidth at each workstation 2 Mbps	Minimum kps (Minimum caching 3 Recommended)  A secure used.  If more testing si proctor o required.
	Linux	Ubuntu 11.10/Fedora 14 <b>(NOTE: Debian 9 / OpenSUSE 11.1 are under review)</b>	Intel Pentium 4 1.0 GHz equivalent or higher performing CPU Recommended Intel Core 2 Duo 1.6 Ghz equivalent or higher performing CPU	Minimum 256MB Free Ram Recommended 512 MB Free Ram	Minimum 1 GB Free Storage Space	Minimum 10" class screen size (10" class is 9.5 to 10.5 inches) Minimum 1024 X 768 screen resolution Recommended 12" or larger screen size	Minimum 100 Mbps LAN/802.11g Wireless 54 Mbps or greater Minimum available LAN bandwidth at each workstation: 1 Mbps Recommended 1 Gbps LAN/802.11n Wireless 150 Mbps or higher Recommended available LAN bandwidth at each workstation 2 Mbps	Minimum kps (Minimum caching 3 Recommended)  A secure used.  If more testing si proctor o required.



## Data Sharing Guidance

November 4, 2014

I. Purpose	89
What is Protected Information?	89
II. Recommendations & Best Practices	90
Data Sharing Agreement Checklist	90
Additional Guidance: (#2) Relevant Laws	91
Additional Guidance: (#3) Aggregate Reporting Rules	93
Additional Guidance: (#6) Suggested Definitions	95
Additional Guidance: (#8), Appropriate Security Measures	97
Additional Guidance: (#7) Data Security Training Best Practices	99
Additional Guidance: (#9) Planning for Breaches of PII	99
Additional Resources	100
IV. References	102
Appendix: Printable Data Sharing Agreement Checklist	104

## I. Purpose

The purpose of this document is to summarize guidance and best practice for written agreements under allowable exceptions as specified in the Family Educational Rights and Privacy Act (FERPA) and Individuals with Disabilities Act (IDEA). Both FERPA and IDEA require states receiving funds from the U.S. Department of Education to protect student information. This requirement extends beyond a state or SEA's employees to include contractors and vendors eligible to work with this data to support state's efforts to improve or enhance education. This document is intended to serve as guidance for member States as they begin sharing protected student data with vendors for field-testing, operational administration, additional development, and score reporting of ELPA21.

### What is Protected Information?

Throughout this document, the terms "protected information", "secure data", "confidential information", and "personally identifiable information (PII)" are used interchangeably.

These terms refer to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

PII includes, but is not limited to the following<sup>3</sup>:

1. The student's name;
2. The name of the student's parent or other family members;
3. The address of the student or student's family;
4. A personal identifier, such as the student's Social Security Number, student number, or biometric record;
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. Academic records, including grades, test scores, courses taken, academic specializations and activities, IEP records, test answer sheets, special education records, and written responses to test questions
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and/or

---

<sup>3</sup> FERPA, 34 CFR § 99.3

7. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

## II. Recommendations & Best Practices

States may have a Data Security & Governance Program in place that identifies and describes expectations for confidential and secure information, including roles and responsibilities, personnel and technical processes for maintaining security, steps contractors are required to take when working with the state’s secure data, and a plan for responding to security breaches. These policies and procedures, including sanctions that the State uses, are required to ensure that its policies and procedures consistent with §§ 300.611 through 300.625 are followed and that the requirements and regulations of IDEA and FERPA are met.

The FERPA Studies Exception, however, allows for the disclosure without consent of personally identifiable information from education records (PII) to organizations conducting studies “for, or on behalf of,” schools, school districts, or postsecondary institutions, including assessment development, delivery, and reporting. IDEA allows for similar disclosure when specific safeguards are met.

### Data Sharing Agreement Checklist

FERPA requires of each state, that once an educational institution discloses protected information to a third party, it is obligated to ensure that the third party does not itself improperly disclose the information in violation of FERPA. The ELPA21 Data Sharing Agreement Checklist below identifies the elements necessary for protecting confidential information as it is shared with contractors.

The checklist is followed by additional information and best practice suggestions pertaining to specific requirements within the checklist that may help to further enhance the expectations and effectiveness of the agreements. *Section III: Additional Resources* provides these additional details for elements noted with an “\*” in the checklist.

To meet the safeguards required under by both FERPA and IDEA, the following checklist identifies the necessary elements of data sharing agreements when PII is involved.

The Appendix includes a one-page printable checklist.

#### ELPA21 Data Sharing Agreement Checklist

<input type="checkbox"/>	<p>1. The State should specify what PII will be disclosed and for what purpose, including the following elements:</p> <ul style="list-style-type: none"> <li>a. purpose of the work,</li> <li>b. scope of the work,</li> <li>c. duration of the work, and</li> </ul>
--------------------------	--

	d. information to be disclosed.
<input type="checkbox"/>	2. *The State should refer to relevant laws, regulations, and rules to which contractor is required to adhere to.
<input type="checkbox"/>	3. *The State should identify limitations on use of the PII, including any methodological or reporting restrictions, such as linking to other data sets, minimum table cell sizes, etc.
<input type="checkbox"/>	4. The State should clearly state ownership of PII.
<input type="checkbox"/>	5. The State should maintain the right to audit, and to review and approve reported results.
<input type="checkbox"/>	6. *The State should include definitions of key terms related to data security.
<input type="checkbox"/>	7. *The State should require the contractor to: <ul style="list-style-type: none"> <li>a. use PII only to meet the purpose(s) of the work,</li> <li>b. limit access to PII to those with legitimate interests; contractor must not allow access to data containing PII to anyone other than authorized employees with legitimate interests in the information,</li> <li>c. provide training to all persons with access to confidential information sufficient to maintain confidentiality of data containing PII,</li> <li>d. maintain, for public inspection, a current listing of the names and positions of those employees within the agency who may have access to PII,</li> <li>e. obtain and keep on file signed affidavits of non-disclosure for all persons with access to secure data, and</li> <li>f. identify an authorized representative to ensure data security and to destroy all PII when the information is no longer needed for the purposes for which this agreement is executed and specify the time period, and destruction methods for each specific type of media (e.g., data wiping, degaussing, shredding, etc.).</li> </ul>
<input type="checkbox"/>	8. *The State should require the contractor to comply with all applicable legal requirements, including maintaining the data in a secure manner by applying appropriate collection, maintenance, use, storage, technical, physical, administrative, and destruction safeguards to properly protect the PII, at rest, during use, and in transit.
<input type="checkbox"/>	9. *The State should require the contractor to have plans that are in accordance with any applicable State and Federal laws for responding to a data breach, including, when appropriate or required, responsibilities and procedures for notification and mitigation, such as: <ul style="list-style-type: none"> <li>a. a time span for reporting (e.g., within one hour of discovery)</li> <li>b. under what circumstances notification to affected individuals or entities is required</li> <li>c. content and means of the notification (e.g. letter, public announcement, email),</li> <li>d. source of the notification (e.g., principal, parent, school board, etc.)</li> <li>e. remediation options</li> <li>f. corrective actions taken, and to be taken.</li> </ul>
<input type="checkbox"/>	10. The State should identify penalties for inappropriate disclosure and security breaches <sup>4</sup> .
<p><i>Checklist adapted from Privacy Technical Assistance Center, U.S. Department of Education, Written Agreement Checklist (2012): <a href="http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf">http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf</a></i></p>	

**Additional Guidance: (#2) Relevant Laws**

Two key pieces of legislation require certain levels of confidentiality with educational data. Both FERPA and IDEA require states and SEAs to implement processes that ensure the security of student data in order to be eligible for federal funds.

<sup>4</sup> The SEA must have in effect the policies and procedures, including sanctions that the State uses, to ensure that its policies and procedures consistent with §§ 300.611 through 300.625 are followed and that the requirements of the Act [IDEA] and the regulations in this part are met.

### **Family Educational and Privacy Rights**

FERPA is a Federal law that is administered by the Family Policy Compliance Office in the U.S. Department of Education (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA applies to all educational agencies and institutions (e.g., schools, districts, states) that receive funding under any program administered by the Department.

FERPA prohibits the disclosure of a student’s “protected information” to a third party. For FERPA, a “third party” includes any individual or organization other than the student or the student’s parent. Even if an initial disclosure of protected information is permissible, FERPA limits the subsequent disclosure of the information by the third party. ***As such, once an educational institution discloses protected information to a third party, it is obligated to ensure that the third party does not itself improperly disclose the information in violation of FERPA.***

FERPA permits an educational agency or institution to disclose PII from the education record of a student without consent if the disclosure meets one or more of the conditions outlined in 20 U.S.C. § 1232g(b) and (h) –(j) and 34 CFR § 99.31. For ELPA21 states, the disclosure of PII from student education records must be for, or on behalf of, an educational agency or institution, in order to:

- a. Develop, validate, or administer predictive tests;
- b. Administer student aid programs; or
- c. Improve instruction.

Regulations require that the educational agency or institution or the State or local educational authority or agency headed by an official listed in 34 CFR §99.31(a)(3) execute a written agreement with the third party when disclosing personally identifiable information from education records without consent. See 34 CFR §99.31(a)(6)(iii)(C).

### **The Individuals with Disabilities Education Act (IDEA) Part B**

IDEA governs special education provision, and related services, and applies to those accepting IDEA funds.

States are eligible for assistance if they submit a plan that provides assurances to the Secretary that the State has in effect policies and procedures to ensure that the State meets each of the following conditions: 1) Procedural safeguards; children with disabilities and their parents are afforded the procedural safeguards required by section 615 and 2) Confidentiality; agencies in the State comply with section 617(c) (relating to the confidentiality of records and information).

### Additional Guidance: (#3) Aggregate Reporting Rules<sup>5</sup>

States may consider requiring contractors to follow guidelines specified in the NCES Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting brief (NCES 2011-603 <http://nces.ed.gov/pubs2011/2011603.pdf>) when displaying student information in public reports. NCES recommends the following rules for data reporting:

- 1) Minimize the enrollment details reported in school, district, and state profiles or in reports of outcome measure results. When possible, provide enrollment data for a different date than that of the reported outcome measures and label the different dates (e.g., fall enrollment for a spring assessment) and tell readers that the data on student enrollment by grade and by selected student characteristics are included to provide context for the results presented but should not be assumed to exactly match the student composition at the time the outcome was measured.
  - a) Report the percentage distribution of students by grade and reporting subgroup at the school, district, or state level in a standalone table without any of the outcome measures or reporting subgroup details.
  - b) Do not report the details of the enrollment data within each reporting subgroup by individual grades.
- 2) Use a minimum of 10 students for the reporting subgroup size limitation.
  - a) Suppress results for all reporting groups with 0 to 9 students.
  - b) Suppress results for reporting subgroups with 0 to 9 students and suppress each of the related reporting subgroups regardless of the number of students in the subgroup (i.e., suppress the other subgroup(s) of the set of subgroups that sum to the overall group). In instances with 3 or more subgroups, the subgroups with 0 to 9 students can be combined with each other or with the smallest reportable subgroup to form an aggregated subgroup of 10 or more students to allow for the reporting of data for larger subgroups.
- 3) Use only whole numbers when reporting the percentage of students for each category of an outcome measure (e.g., the percentage assessed).
- 4) Do not report the underlying counts for the subgroup or group totals (i.e., the denominators of the percentages); also do not report the underlying counts of students in individual outcome categories (i.e., the numerators).
- 5) In the remaining reporting groups and subgroups that are related (i.e., groups that in combination sum to the total):
  - a) For reporting variables/outcome measures with more than 300 students and no related subgroup with fewer than 200 students, use the following approach:
    - i) Recode categories with values of 99 to 100 percent to greater than or equal to 99 percent ( $\geq 99$  percent).

---

<sup>5</sup> Adapted from Education Sciences SLDS Technical Brief 3, Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603), <http://nces.ed.gov/pubs2011/2011603.pdf>.

- ii) Recode categories with values of 0 to 1 percent to less than or equal to 1 percent ( $\leq 1$  percent).
  - iii) Otherwise, report the percentage of students in each category using whole numbers.
- b) For reporting variables/outcome measures with 201 to 300 students and no related subgroup with fewer than 200 students, use the following approach:
- i) Recode categories with values of 98 to 100 percent to greater than or equal to 98 percent ( $\geq 98$  percent).
  - ii) Recode categories with values of 0 to 2 percent to less than or equal to 2 percent ( $\leq 2$  percent).
  - iii) Otherwise, report the percentage of students in each category using whole numbers.
- c) For reporting variables/outcome measures in which the number of students ranges from 101 to 200, use the following option in this group and all related subgroups with more than 200 students:
- i) Recode categories with values of 98 to 100 percent to greater than or equal to 98 percent ( $\geq 98$  percent).
  - ii) Recode categories with values of 0 to 2 percent to less than or equal to 2 percent ( $\leq 2$  percent).
  - iii) Recode the percentage in each remaining category in all reporting groups or subgroups to intervals as follows (3–4, 5–9, 10–14, 15–19, . . . , 85–89, 90–94, 95–97).
- d) For reporting variables/outcome measures in which the number of students in the smallest reporting group or subgroup ranges from 41 to 100, use the following option in that group or subgroup and use option 5c for each related reporting group or subgroup with more than 100 students:
- i) Recode categories with values of 95 to 100 percent to greater than or equal to 95 percent ( $\geq 95$  percent).
  - ii) Recode categories with values of 0 to 5 percent to less than or equal to 5 percent ( $\leq 5$  percent).
  - iii) Recode the percentage in each remaining category in all reporting groups or subgroups to intervals as follows (6–9, 10–14, 15–19, 20–24, . . . , 85–89, 90–94).

Modifications to secure data files and fields removing PII provide additional security, Although the lack of precision makes these techniques less applicable to high-stakes testing, they may be useful in system testing. Anonymizing techniques include<sup>6</sup>:

- Generalizing the Data—Making information less precise, such as grouping continuous values
- Suppressing the Data—Deleting an entire record or certain parts of records

---

<sup>6</sup> Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Recommendations of the National Institute of Standards and Technology, p4-5.

- Introducing Noise into the Data—Adding small amounts of variation into selected data
- Swapping the Data—Exchanging certain data fields of one record with the same data fields of another similar record (e.g., swapping the ZIP codes of two records)
- Replacing Data with the Average Value—Replacing a selected value of data with the average value for the entire group of data.

### Additional Guidance: (#6) Suggested Definitions

States may consider using the following definitions in data sharing agreements.

**Affidavit of Nondisclosure**<sup>7</sup>. A brief form that is completed by any person who may have access to individually identifiable information. This form should contain: (1) the name of the database(s) to be accessed, (2) the wording of an oath not to disclose such information to persons not similarly sworn, (3) a description of the penalties for such disclosure, and (4) the imprint of a notary public.

**Anonymization**<sup>8</sup> [of data] refers to the process of data de-identification which produces de-identified data, where individual records cannot be linked back to an original student record system or to other individual records from the same source, because they do not include a record code needed to link the records. As such, anonymized data are not useful for monitoring the progress and performance of individual students; however, they can be used for other research or training purposes. An anonymized data file could be produced from the de-identified file that contains record codes by removing the codes and reviewing the resulting file to ensure that additional disclosure limitation methods do not need to be applied. The documentation for the anonymized data file should identify any disclosure limitation techniques that were applied and their implications for the analysis.

**Blurring**<sup>9</sup> is a disclosure limitation method which is used to reduce the precision of the disclosed data to minimize the certainty of individual identification. There are many possible ways to implement blurring, such as by converting continuous data elements into categorical data elements (e.g., creating categories that subsume unique cases), aggregating data across small groups of respondents, and reporting rounded values and ranges instead of exact counts to reduce the certainty of identification. Another approach involves replacing an individual's actual reported value with the average group value; it may be performed on more than one variable with different groupings for each variable.

---

<sup>7</sup> While vendor agreements may typically cover employees, requiring each individual to sign an affidavit of nondisclosure clarifies the responsibilities of and accountability for each individual, and may reduce the number of individuals provided with access to the data, and the likelihood that confidential data may be shared between colleagues.

<sup>8</sup> Privacy Technical Assistance Center, Data De-identification: An Overview of Basic Terms, p2.

<sup>9</sup> Privacy Technical Assistance Center, Data De-identification: An Overview of Basic Terms, p2.

**Confidentiality**<sup>10</sup> relates to the management of another individual's personally identifiable information.

**Data Security**<sup>11</sup>. Security refers to protecting personally identifiable information (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

**De-identification**<sup>12</sup> [of data] refers to the process of removing or obscuring any personally identifiable information from student records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them. Specific steps and methods used to de-identify information (see disclosure limitation method for details) may vary depending on the circumstances, but should be appropriate to protect the confidentiality of the individuals. While it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is no reasonable basis to believe that the remaining information in the records can be used to identify an individual.

**Disclosure**<sup>13,14</sup>

Disclosure means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record. Disclosure also occurs when a data subject is identified from a released file (*identity disclosure*), sensitive information about a data subject is revealed through the released file (*attribute disclosure*), or the released data make it possible to determine the value of some characteristic of an individual more accurately than otherwise would have been possible (*inferential disclosure*).

**Encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when it is stored on a transportable magnetic medium.

**Personally identifiable information (PII)**<sup>15,16</sup>. Educational Records protected under FERPA are those containing personal information, family information, and/or academic information. PII includes, but is not limited to 1) student name, 2) parent or other family

---

<sup>10</sup> Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records, p6.

<sup>11</sup> Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records, p8.

<sup>12</sup> Privacy Technical Assistance Center, Data De-identification: An Overview of Basic Terms, p2.

<sup>13</sup> IDEA And FERPA Confidentiality Provisions, p9.

<sup>14</sup> Report of the Committee on National Statistics' Panel on Confidentiality and Data Access, Duncan et al., 1993. Private Lives and Public Policies, Washington, DC: National Academy Press, p. 23.

<sup>15</sup> Data Sharing Agreement Checklist, p6

<sup>16</sup> Protecting The Privacy Of Student Records: Guidelines for Education Agencies

members, 3) address, 4) personal identifier, such as the student’s Social Security Number or student number, 5) date or place of birth, 6) academic records, including grades, test scores, courses taken, academic specializations and activities, IEP records, test answer sheets, special education records, and responses to test questions, 7) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and/or 7) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

**Secure Data.** Secure data contains personally identifiable or confidential information.

### Additional Guidance: (#8), Appropriate Security Measures

Consider implementing the following expectations for data sharing agreements to ensure protection of PII.

#### **Technology Security Measures**

Consider requiring contractor to adhere to technical requirements in most recently updated versions of NCES’ Privacy Technical Assistance Center’s Data Security Checklist and the security standards described by the National Institute of Standards and Technology. Key security features include, but are not limited to the following:

- Automatic lockout on computers storing secure data after more than 3 failed login attempts,
- Login required on computers storing secure data after a period of inactivity (2-3 minutes),
- Maintain and audit access logs for secure files for weekly review of suspicious login activity.
- Utilize strong passwords on computers and file containing secure data:
  - at least 8 characters,
  - include numeric and alphanumeric characters, uppercase and lowercase characters, and special characters,
  - disallow any version of “password”
  - disallow passwords containing elements of the user’s login or name
  - require passwords to secure data files to be changed on a regular basis.
- Establish secure data backup policies (i.e., can it be backed up, and to where.)
- Establish secure data remote access, networked computer, and portable computer policies.
- Establish secure data transfer policies (can it be encrypted and emailed?).
- Overwrite, rather than delete, secure data by saving new data in the file storage location to make deleted secure data unreadable.

- Require secure data to be encrypted when stored on servers or on mobile devices, such as laptops, smart phones, external hard drives, and thumb drives.
- Specify that all secure data provided to the third party must be destroyed when no longer needed for the specific purpose for which it was provided, including any copies of the PII that may reside in system backups, portable devices, temporary files, or other storage media.
  - Be specific in the written agreement as to the type of destruction to be carried out. Consider incorporating data destruction best practices provided by the US Department of Education's Privacy Technical Assistance Center into data sharing agreements. Access at: <http://ptac.ed.gov/sites/default/files/Best Practices for Data Destruction %282014-05-06%29 %5BFinal%5D.pdf>.
  - Require secure data files to be overwritten, not deleted, when a computer containing restricted-use data is no longer used (e.g., reallocated to other projects), the computer needs to be repaired (e.g., hard disk crashes), or the project ends.
  - Ensure accountability for destruction of PII by using certification forms which are signed by the individual responsible for performing the destruction and contain detailed information about the destruction.
- Additional advanced technical guidance exists for network, hardware, and IT system security. Refer to The National Institute of Standards and Technology's *Guide to Protecting Confidentiality of Personally Identifiable Information (PII)* at [csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf](https://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf) or the Federal Information Processing Standards Publication 140-2, *Security Requirements For Cryptographic Modules* at [csrc.nist.gov/groups/STM/cmvp/standards.html](https://csrc.nist.gov/groups/STM/cmvp/standards.html), or the Privacy Assistance Technical Assistance Center's *Data Security Checklist* at [ptac.ed.gov/sites/default/files/ptac-data-security-checklist.pdf](http://ptac.ed.gov/sites/default/files/ptac-data-security-checklist.pdf) for these additional technical security measures.

### **Federal Information Processing Standards**

ELPA21 States should consider requiring that portable devices used by contractors, such as laptops and thumb drives, containing secure data satisfy a level of FIPS 140-2 (Federal Information Processing Standard, Publication 140-2)<sup>17</sup>. FIPS 140-2 isn't a technology, but a definition of what security mechanisms are necessary to protect portable data and who is authorized to access the data. The four levels described by FIPS 140-2 are below. Level 2 should sufficiently address State data security needs<sup>18</sup>.

FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" and use an approved encryption algorithm

---

<sup>17</sup> Accessible at <http://www.nist.gov/itl/fipscurrent.cfm>

<sup>18</sup> Manufacturers such as Kingston and Iron Key offer FIPS Level 2 certified flash drives on Amazon and other retailers. FIPS compliant drives are more costly than regular drives, and the cost increases with each additional level of security. Certified Level 2 devices can be found for \$80-\$150.

(e.g., 256-bit AES hardware encryption) and various kinds of insecurity must be absent.

FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication. For certified level two devices, if someone tries to physically open the drive to access encryption keys, it will show evidence of tampering.

FIPS 140-2 Level 3 adds requirements for physical tamper-resistance and identity-based authentication (such as requiring a fingerprint or passcode to enter the encryption key) . In level three devices, the encryption keys to unlock the data are destroyed if someone tries to physically get into the drive to bypass them.

FIPS 140-2 Level 4 adds requirements to make the physical security requirements more stringent, and requires robustness against environmental attacks. Level 4 devices are designed for use in physically unprotected environments, and destroy the encrypted data and the encryption keys if physically tampering occurs.

### **Workspace Security Measures**

- Require computer rooms/areas that process secure data must be secure during business hours and doors and windows locked after close of business or when vacant.
- Require printed material containing individually identifiable information shall always be secured from unauthorized access (e.g., locked in a secure location when not in use, turned face down when unauthorized individuals approach workspace).
- Require non-electronic secure data to be destroyed when no longer needed for the purpose for which it was disclosed. Commonly used methods include cross-cut shredders, pulverizers, and incinerators.

### **Additional Guidance: (#7) Data Security Training Best Practices**

Consider incorporating data security best practices outlined by the Privacy Technical Assistance Center into state policies and practices and expectations for contractors described by state data sharing agreements. For best practices in security training, please see <http://ptac.ed.gov/sites/default/files/issue-brief-security-training.pdf>.

### **Additional Guidance: (#9) Planning for Breaches of PII**

FERPA requires educational agencies and institutions to record all disclosures of PII from education records to organizations made under the studies exception (§ 99.32). The NIST 2010 Guide (Special Publication 800-122, pg. 5-1, 2) recommends that if a breach occurs, the report should include the following information:

1. Name, job title, and contact information of the person reporting the incident;
2. Name, job title, and contact information of the person who discovered the incident;
3. Date and time the incident was discovered;

4. Nature of the incident (e.g., system level electronic breach, an electronic breach of one computer or device, or a breach of paper extracts of records);
5. Description of the information lost or compromised;
6. Name of electronic system and possible interconnectivity with other systems;
7. Storage medium from which information was lost or compromised;
8. Controls in place to prevent unauthorized use of the lost or compromised information;
9. Remedial controls to be put in place to prevent future unauthorized use of the lost or compromised information, and;
10. Number of individuals potentially affected.

States are advised to have policies identifying penalties for unauthorized access or security breaches.

### Additional Resources

Below are several links that provide more detailed discussions on requirements and best practices that may be helpful to states in creating or updating data security processes, including those necessary for inclusion in data sharing agreements for data containing PII.

Helpful organizations and resources:

- US Department of Education, Privacy Technical Assistance Center (PTAC): <http://ptac.ed.gov>
- National Center for Educational Statistics (NCES): <http://nces.ed.gov/>
- National Institute of Standards and Technology (NIST): <http://csrc.nist.gov>
- Federal regulations resources webpage at the U.S. Department of Education: <http://www.ed.gov/policy/gen/reg/edpicks.ihtml?src=ln>.

Data Governance:

- *Data Stewardship: Managing Personally Identifiable Information in Student Education Records* (NCES 2011--602): <http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602>.
- National Forum on Education Statistics (2004). *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies*, (NCES 2004-330). Washington, DC: <http://nces.ed.gov/pubs2004/2004330.pdf>.
- National Forum on Education Statistics (2004). *Forum Guide to Building a Culture of Quality Data: A School & District Resource*, (NFES 2005-801). Washington, DC: <http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2005801>.
- *Data Governance Checklist*: <http://ptac.ed.gov/toolkit>.
- *Written Agreement Checklist* (2012): <http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf>.

Technical and Procedural Data Security:

- *Data Security Checklist*: <http://ptac.ed.gov/toolkit>.
- *Best Practices for Data Destruction*: <http://ptac.ed.gov/document/best-practices-data-destruction>.
- *PTAC Issue Brief Data Security: Top Threats to Data Protection*: [http://ptac.ed.gov/toolkit\\_data\\_security](http://ptac.ed.gov/toolkit_data_security).
- National Institute of Standards and Technology (NIST), *Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication (FIPS PUB) 199* (2004): <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.
- McCallister, E., Grance, T., and Scarfone, K. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-122)*. National Institute of Standards and Technology, U.S. Department of Commerce. Washington, DC: <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.
- *System Administration, Networking, and Security Institute, 20 Critical Security Controls* (Version 5): <https://www.sans.org/critical-security-controls/>.

Data Security in Analysis and Reporting

- Statewide Longitudinal Data Systems (SLDS, 2010), *Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting*. Issue Brief 3, NCES 2011-603, <http://nces.ed.gov/pubs2011/2011602.pdf>.

## IV. References

Duncan et al., (1993). American Statistical Association, Committee on Privacy and Confidentiality, *Key Terms/Definitions in Privacy and Confidentiality*. Alexandria, VA. <http://www.amstat.org/committees/pc/keyterms.html>.

Family Policy Compliance Office, U.S. Department of Education: *Guidance for Reasonable Methods and Written Agreements* (2011): [http://www.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd\\_agreement.pdf](http://www.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf).

Federal Register, Part II Department of Education. Family Educational Rights and Privacy; Final Rule (34 CFR Part 99). Washington, DC: Vol. 73, No. 237. Tuesday, December 9, 2008.

FERPA regulations amendment released in 2011: <http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf>.

Statewide Longitudinal Data Systems (SLDS, 2010), *Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting*. Issue Brief 3, NCES 2011-603, <http://nces.ed.gov/pubs2011/2011602.pdf>.

National Center for Educational Statistics, *Data Stewardship: Managing Personally Identifiable Information in Student Education Records*. Accessed from <http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602>.

National Forum on Education Statistic (2004). *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies*, (NCES 2004-330). Washington, DC: <http://nces.ed.gov/pubs2004/2004330.pdf>.

National Forum on Education Statistic (2004). *Forum Guide to Building a Culture of Quality Data: A School & District Resource*, (NFES 2005-801). Washington, DC: <http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2005801>.

National Institute of Standards and Technology (NIST), *Data Sharing Checklist*: <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>.

National Institute of Standards and Technology (NIST), *NIST SP 800-14 (Generally Accepted Principles and Practices for Securing Information Technology Systems)*: <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>.

Office of Management and Budget (2007). OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf>.

Privacy Technical Assistance Center, U.S. Department of Education, *Best Practices for Data Destruction*: <http://ptac.ed.gov/document/best-practices-data-destruction>.

Privacy Technical Assistance Center, U.S. Department of Education, *Data Governance Checklist*: <http://ptac.ed.gov/toolkit>.

Privacy Technical Assistance Center, U.S. Department of Education, (2014). *FERPA Exceptions Summary*, <http://ptac.ed.gov/toolkit>.

Privacy Technical Assistance Center, U.S. Department of Education, *Data De-identification: An Overview of Basic Terms*: [http://ptac.ed.gov/sites/default/files/data\\_deidentification\\_terms.pdf](http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf).

Privacy Technical Assistance Center, U.S. Department of Education, *FERPA/IDEA Cross-Walk*: <http://ptac.ed.gov/toolkit>.

Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): <http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf>.

Report of the Committee on National Statistics' Panel on Confidentiality and Data Access, (1993). *Private Lives and Public Policies*, Washington, DC: National Academy Press.

Statewide Longitudinal Data Systems (SLDS) Technical Brief 2. Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records (NCES 2011-602): <http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602>.

U.S. Code, Title 20—Education, Chapter 31—General Provisions Concerning Education, Subchapter III—General Requirements and Conditions Concerning Operation and Administration of Education Programs: General Authority of Secretary, Part 4—Records, Privacy, Limitation on Withholding Federal funds, Section 1232g. Family Educational and Privacy Rights, (20USC1232g). Washington, DC: GPO Access. <http://frwebgate4.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=799486197532+0+1+0&WAISSaction>.

U.S. Department of Commerce, National Institute of Standards and Technology (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, (SP 800-122). Gaithersburg, MD.

## Appendix: Printable Data Sharing Agreement Checklist

<input type="checkbox"/>	1. The State should specify what PII will be disclosed and for what purpose, including the following elements: <ol style="list-style-type: none"> <li>a. purpose of the work,</li> <li>b. scope of the work,</li> <li>c. duration of the work,</li> <li>d. and information to be disclosed.</li> </ol>
<input type="checkbox"/>	2. *The State should refer to relevant laws, regulations, and rules to which contractor is required to adhere to.
<input type="checkbox"/>	3. *The State should identify limitations on use of the PII, including any methodological or reporting restrictions, such as linking to other data sets, minimum table cell sizes, etc. Consider requiring the contractor to follow guidelines specified in the Institute of Education Sciences SLDS Technical Brief 3, Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603 <a href="http://nces.ed.gov/pubs2011/2011603.pdf">http://nces.ed.gov/pubs2011/2011603.pdf</a> ) when displaying student information in public reports.
<input type="checkbox"/>	4. The State should clearly state ownership of PII.
<input type="checkbox"/>	5. The State should maintain the right to audit, and to review and approve reported results.
<input type="checkbox"/>	6. *The State should include definitions of key terms related to data security.
<input type="checkbox"/>	7. The State should require the contractor to: <ol style="list-style-type: none"> <li>a. use PII only to meet the purpose(s) of the work,</li> <li>b. limit access to PII to those with legitimate interests, contractor must not allow access to data containing PII to anyone other than authorized employees with legitimate interests in the information,</li> <li>c. provide training to all persons with access to confidential information sufficient to maintain confidentiality of data containing PII,</li> <li>d. maintain, for public inspection, a current listing of the names and positions of those employees within the agency who may have access to personally identifiable information,</li> <li>e. obtain and keep on file signed affidavits of non-disclosure for all persons with access to secure data,</li> <li>f. identify an authorized representative to ensure data security and to destroy all PII when the information is no longer needed for the purposes for which this agreement is executed and specify the time period, and destruction methods for each specific type of media (e.g., data wiping, degaussing, shredding, etc.).</li> </ol>
<input type="checkbox"/>	8. *The State should require the contractor to comply with all applicable legal requirements, including maintaining the data in a secure manner by applying appropriate collection, maintenance, use, storage, technical, physical, administrative, and destruction safeguards to properly protect the PII, at rest, during use, and in transit.
<input type="checkbox"/>	9. *The State should require the contractor to have plans that are in accordance with any applicable State and Federal laws for responding to a data breach, including, when appropriate or required, responsibilities and procedures for notification and mitigation, such as: <ol style="list-style-type: none"> <li>a. a time span for reporting (e.g., within one hour of discovery)</li> <li>b. under what circumstances notification to affected individuals or entities is required</li> <li>c. content and means of the notification (e.g. letter, public announcement, email),</li> <li>d. source of the notification (e.g., principal, parent, school board, etc.)</li> <li>e. remediation options</li> <li>f. corrective actions taken, and to be taken.</li> </ol>
<input type="checkbox"/>	10. The State should identify penalties for inappropriate disclosure and security breaches.
<p><i>Checklist adapted from Privacy Technical Assistance Center, U.S. Department of Education, Written Agreement Checklist (2012): <a href="http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf">http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf</a></i></p>	

APPENDIX E

ELL POPULATION BY STATE AND GRADE

	AR 2012- 2013	IA 2013- 2014	KS 2011- 2012	LA	NE 2012- 2013	OH 2011- 2012	OR 2012- 2013	SC 2013- 2014	WA 2011- 2012	WV 2013- 2014	
<b>Total for reported year</b>	34114	25275	46956	13042	18009	40231	53597	41038	89152	2516	
<b>K</b>	7611	3198	5110		2562	4418	15824	4669	15371	213	
<b>1</b>		3083	5053		5507	5418		4839	14671	235	
<b>2</b>	6570	2925	4905				5001	14255	4661	11817	218
<b>3</b>		2724	4825			4859	4316		8363	203	
<b>4</b>	6267	2513	4502		4893	4052	10855	3968	7429	186	
<b>5</b>		2228	4233					3220	3633	6494	203
<b>6</b>	7345	1815	3953		1991	2473	6868	3137	5468	185	
<b>7</b>		1497	3490					2209	2766	4402	184
<b>8</b>		1385	3013					2063	2591	3603	180
<b>9</b>	6321	1196	2770		2052	2337	5795	2665	3994	198	
<b>10</b>		994	2292					1571	1721	2985	175
<b>11</b>		906	1603					1460	1206	2405	159
<b>12</b>		799	1207					1150	866	2150	108
Number of Title III students who took the state annual ELPA*	4548	4627	1844	4424	4887	9880	11056	7193	23674	198	
<b>CFR Total*</b>	32814	22425	47040	13952	20304	42824	58580	38553	97397	1865	

\*Consolidated Federal Reporting (2011-12)

APPENDIX F

TABLE OF TOP LANGUAGES OTHER THAN ENGLISH - CONSORTIUM

<b>Language</b>	<b># of ELLs reporting language use/language background</b>
Spanish	
Vietnamese	
Russian	
Arabic	
Chinese (which?)	
Somali	
Ukrainian	
Korean	
Tagalog	
Bosnian	

APPENDIX G

TABLE OF TOP LANGUAGES OTHER THAN ENGLISH – by state

	AR	IA	K S	L A	NE	OH	OR	SC	WA	WV
Language	Spanish	Spanish (Castilian)			Spanish	Spanish	Spanish (Universal)	Spanish (Mexican)	Spanish	Spanish (non-specified)
Percent	43.7	70			67	35	77.2		64	61
Language	Marshallese	Vietnamese			Karen	Somali	Russian	Russian	Russian	Arabic
Percent	3	4			5.2	8	3.5		4.2	14
Language	Vietnamese	Bosnian			Arabic	Arabic	Vietnamese	Vietnamese	Vietnamese	Mandarin
Percent	< 1	3			3	7	2.8		3.7	10
Language	Lao	Karen Languages			Vietnamese	Chinese (non-specified)	Chinese (non-specified)	Arabic	Somali	Vietnamese
Percent	< 1	2			2.5	2	1.7		2.1	5
Language	Hmong	Arabic			Somali	Japanese	Arabic	Mandarin	Korean, Arabic	Cantonese
Percent	< 1	1			1.7	2	1.4		1.3	3