ASEBA
Achenbach
System of
Empirically
Based
Assessment

Version: 1.1
Last Updated: December 1st, 2022

General Information on ASEBA-PC™ Security and Compliance

Systems Overview

ASEBA-PC™ is a standalone implementation that resides on a single workstation and does not communicate with any server or resource that resides outside of that single workstation. Within ASEBA-PC™ itself, the data is encrypted twice, once at the application level and once at the database level. These two levels of encryption at rest have separate 256-bit encryption keys.

The purpose of ASEBA-PC™ is to facilitate the collection of behavioral data regarding a patient receiving or about to receive care and convert it into an actionable assessment of the patient's current behavioral state. ASEBA-PC™ does this by applying the principals of the Achenbach System of Empirical Behavioral Assessment (ASEBA®) to the data, creating what is called a "scored report". A page from scored report might look like the following:
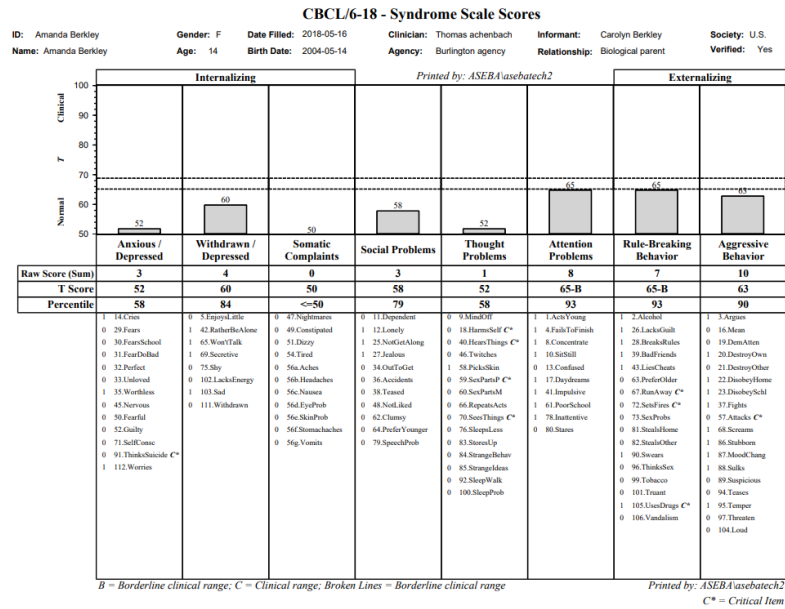
The data needed to produce this report comes from a standard set of ASEBA® forms. There are two principal ways that a form can be entered into ASEBA-PC™:

- Informants can fill out paper forms. The answers to those paper forms can be transcribed directly into ASEBA-PC™ using the "Key Entry" function.

- Form answers stored electronically elsewhere can be formatted into a special text file format and imported into the system using the "Import" function.

The following is an example of a paper form:

Please print. Be sure to answer all items.

Below is a list of items that describe children and youths. For each item that describes your child *now or within the past 6 months*, please circle the *2* if the item is *very true or often true* of your child. Circle the *1* if the item is *somewhat or sometimes true* of your child. If the item is *not true* of your child, circle the *0*. Please answer all items as well as you can, even if some do not seem to apply to your child.

0 = Not True (as far as you know)   1 = Somewhat or Sometimes True   2 = Very True or Often True

0 1 2	1. Acts too young for his/her age	0 1 2	32. Feels he/she has to be perfect
0 1 2	2. Drinks alcohol without parents' approval (describe):	0 1 2	33. Feels or complains that no one loves him/her
0 1 2	3. Argues a lot	0 1 2	34. Feels others are out to get him/her
0 1 2	4. Fails to finish things he/she starts	0 1 2	35. Feels worthless or inferior
0 1 2	5. There is very little he/she enjoys	0 1 2	36. Gets hurt a lot, accident-prone
0 1 2	6. Bowel movements outside toilet	0 1 2	37. Gets in many fights
0 1 2	7. Bragging, boasting	0 1 2	38. Gets teased a lot
0 1 2	8. Can't concentrate, can't pay attention for long	0 1 2	39. Hangs around with others who get in trouble
0 1 2	9. Can't get his/her mind off certain thoughts; obsessions (describe):	0 1 2	40. Hears sound or voices that aren't there (describe):
0 1 2	10. Can't sit still, restless, or hyperactive	0 1 2	41. Impulsive or acts without thinking
0 1 2	11. Clings to adults or too dependent	0 1 2	42. Would rather be alone than with others
0 1 2	12. Complains of loneliness	0 1 2	43. Lying or cheating
0 1 2	13. Confused or seems to be in a fog	0 1 2	44. Bites fingernails
0 1 2	14. Cries a lot	0 1 2	45. Nervous, highstrung, or tense
0 1 2	15. Cruel to animals	0 1 2	46. Nervous movements or twitching (describe):
0 1 2	16. Cruelty, bullying, or meanness to others		
0 1 2	17. Daydreams or gets lost in his/her thoughts	0 1 2	47. Nightmares
0 1 2	18. Deliberately harms self or attempts suicide	0 1 2	48. Not liked by other kids
0 1 2	19. Demands a lot of attention	0 1 2	49. Constipated, doesn't move bowels
0 1 2	20. Destroys his/her own things	0 1 2	50. Too fearful or anxious
0 1 2	21. Destroys things belonging to his/her family or others	0 1 2	51. Feels dizzy or lightheaded
0 1 2	22. Disobedient at home	0 1 2	52. Feels too guilty
0 1 2	23. Disobedient at school	0 1 2	53. Overeating
0 1 2	24. Doesn't eat well	0 1 2	54. Overtired without good reason
0 1 2	25. Doesn't get along with other kids	0 1 2	55. Overweight
0 1 2	26. Doesn't seem to feel guilty after misbehaving		56. Physical problems *without know medical cause*:
0 1 2	27. Easily jealous	0 1 2	a. Aches or pains (*not* stomach or headaches)
0 1 2	28. Breaks rules at home, school, or elsewhere	0 1 2	b. Headaches
0 1 2	29. Fears certain animals, situations, or places, other than school (describe):	0 1 2	c. Nausea, feels sick
		0 1 2	d. Problems with eyes (*not* if corrected by glasses) (describe):
0 1 2	30. Fears going to school	0 1 2	e. Rashes or other skin problems
0 1 2	31. Fears he/she might think or do something bad	0 1 2	f. Stomachaches
		0 1 2	g. Vomiting, throwing up
		0 1 2	h. Other (describe):

PAGE 3   *Be sure you answered all items Then see other side.*

With the information in the scored report, a clinician can make informed decisions regarding that patient's care. In addition, ASEBA-PC™ contains functions to assist in the workflow of getting forms filled out, and functions for the export of data in bulk for research purposes by the customer.

RCCYF employees have no direct access to any customer data stored in ASEBA-PC™. Our support policies prohibit remote access to customer workstations except in a screenshare with an authorized customer representative. Additionally, we cannot access the database directly in readable form in the backend due to the two-layer encryption we use. This restriction includes any sensitive patient data, such as what may be classified as PHI in the United States.

Even if a customer determines they need to share screens for remote access, PHI can be protected. ASEBA-PC™ contains a switch that allows users to hide sensitive patient data in the UI so even in the instance RCCYF employees were asked to view ASEBA-PC™ we could still not see your sensitive patient data.

In general, our employees are trained to avoid contact with any customer data. RCCYF employees will not open emails or attachments from customers unless they are certain that those items do not contain PHI. Any clinical data accidentally sent to us, whether electronically or in paper format is destroyed per our media handling policy.

Use of Subcontractors in ASEBA-PC™

The RCCYF does not use subcontractors in the support and maintenance of ASEBA-PC™. All personnel involved are under the direct employ of the RCCYF, and reside in the United States.

Access Control

Access control to ASEBA-PC™ is through user accounts. User accounts that are designated as "Administrator" have the privileges in the system to create and manage other user accounts. User accounts can be activated to allow access and deactivated to restrict access.

Control of data directly into the ASEBA-PC™ database is severely restricted. Due to the presence of application-layer encryption, only valid user accounts have the proper access rights necessary to read data stored in the ASEBA-PC™ database. Any attempt at a direct query to the database will return encrypted and unreadable data, even if the direct query provides the proper database-level decryption key.

Identification and Authorization

ASEBA-PC™ uses an internal authentication policy, which validates username and password. Users are authenticated at login into ASEBA-PC™, and that login event is limited to the single instance of ASEBA-PC™ on that workstation.

Passwords have length and complexity rules associated with them, and also expire after a designated period of time.

Awareness and Training

As per our policies regarding compliance with all jurisdictions where ASEBA-PC™ is offered, all RCCYF employees undergo annual information security and awareness training. This training includes understanding of the compliance environment where we sell our products, including HIPAA in the United States and GDPR in the European Union. Our technical team has additional training and guidelines on proper data security in product development and support. The RCCYF keeps full training records for all of its employees.

Audit and Accountability

ASEBA-PC™ logs audit events of all user actions taken within the software. All logs are read-only and cannot be edited by a user. Logged events do not contain any clinical data, including PHI. Logged events do contain all information pertaining to the user interaction, including appropriate timestamps, user identifiers, and the action taken by the user.

These logs are available at any time to users of ASEBA-PC™. Logs are kept indefinitely unless purged by the customer through access granted to a user with the "Administrator" role.

Certification, Accreditation and Security Assessments

The RCCYF takes a proactive approach to assessing risk in our product development, and uses third party products to conduct regular vulnerability and penetration testing. More information on our vulnerability testing and penetration testing, including recent test results, is available on request.

The RCCYF regularly undergoes a 3rd-party audit to certify our compliance with HIPAA. Our most recent attestation of HIPAA compliance is available on request. As RCCYF does not have access to customer PHI stored in ASEBA-PC™, the most important aspects of HIPAA compliance surround our customer service and support procedures.

System and Communications Protection

Data stored in ASEBA-PC™ does not leave the workstation where ASEBA-PC™ is installed.

By policy, the RCCYF does not accept any files from customers that are suspected of containing protected patient data. Transfer of files in general are not a common occurrence with ASEBA-PC™ customers, but if necessary we utilize a secure transfer file system to do so.

Configuration Management

The customer is responsible for configuration and patch management for their ASEBA-PC™ implementation.

Contingency Planning

ASEBA-PC™ is installed on a customer-owned workstation, and all contingency planning and execution of data backups are the responsibility of the customer.

Incident Response

The RCCYF maintains a full incident response process and policy. However, data in ASEBA-PC™ is not accessible by RCCYF employees or is transferred to our systems.

Maintenance

ASEBA-PC™ is installed on a customer-owned workstation, and all maintenance tasks are the responsibility of the customer.

Media Protection

The RCCYF maintains a full media protection and disposal policy. However, data in ASEBA-PC™ is not accessible by RCCYF employees or is transferred to our systems.

Physical and Environmental Protection

As ASEBA-PC™ is installed on a customer-owned workstation, the customer is responsible for all physical and environmental protection requirements.

Planning

Information security is included in overall business planning, as all of the RCCYF's software products require the use and storage of sensitive patient data. Security items are not documented in a separate plan document, but are incorporated into the development planning documents as the software is built and maintained.

Personnel Security

All RCCYF employees carry ID badges. The RCCYF conducts 3rd-party screening of employees. Upon termination, all employee access to RCCYF systems are deactivated.

Risk Assessments

Risk assessments are performed as part of the development process for new features. Vulnerability assessments and testing are performed on a regular basis, both during development and also after deployment.

System and Information Integrity

Developers of ASEBA-PC™ engage in secure coding practices. All code is formally reviewed for security concerns at points both in the development and deployment of software. Tests for input validation and malicious code insertion are standard and conducted with every build.

Revision History

Version	Date of Revision	Author	Description of Changes
1.0	April 10th, 2020	David Deforge	Initial version.
1.1	December 1st, 2022	David Deforge	Format and presentation changes.