PARiConnect Privacy Policy

Effective Date: January 1, 2020

Contents

Psychological Assessment Resources, Inc. ("**PAR**") understands the importance of protecting the confidentiality and privacy of information concerning your clients. The PARiConnect Privacy Policy ("**Policy**") explains PAR's information collection practices with respect to

information submitted at or through the PARiConnect platform at https://www.pariconnect.com ("**PARiConnect**"). This Policy applies only to information collected through PARiConnect.

California Residents

For residents of California, effective January 1, 2020, please refer to our California Privacy Policy for additional information concerning your rights about the personal information we collect, use, and disclose. To the extent this Notice in any way conflicts with the California Privacy Policy, the California Privacy Policy controls.

Definitions

For purposes of this Policy, the following terms have the corresponding definitions:

1. **"Business Associate"** has the meaning specified in the Privacy Rule, the Security Rule, and § 27938 of the HITECH Act, particularly 45 C.F.R. § 160.103;
2. **"Individual"** has the meaning specified in 45 C.F.R. § 160.103;
3. **"Client"** means an Individual whose PHI is processed via PARiConnect on behalf of the Customer, whether such Individual is a client, patient, or student;
4. **"Covered Entity"** has the meaning specified in 45 C.F.R. § 160.103;
5. **"Customer"** means a PAR customer who has registered to use PARiConnect;
6. **"DHHS"** means the United States Department of Health and Human Services;
7. **"Directory Information,"** "Educational Agency or Institution," "Education Records," and "Student" have the meanings specified in 34 C.F.R. § 99.3;
8. **"Electronic Protected Health Information,"** or "ePHI," has the meaning specified in 45 C.F.R. § 160.103;
9. **"FERPA"** means the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g;
10. **"FERPA Regulations"** mean the regulations found at 34 C.F.R. Part 99;
11. **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996;
12. **"HITECH Act"** means the Health Information Technology for Economic and Clinical Health Act of 2009;
13. **"PAR"** means Psychological Assessment Resources, Inc., 16204 North Florida Avenue, Lutz, FL, 33549;

14. **"PAR Employees"** includes all PAR employees, consultants, trainees, agents, and other persons whose work performance is under PAR's direct control, whether or not they are paid by PAR;
15. **"PARiConnect"** means the online, automated computer assessment platform with web-based access located at https://www.pariconnect.com;
16. **"Privacy Rule"** means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, subparts A and E;
17. **"Protected Health Information,"** or "PHI," has the meaning specified in 45 C.F.R. § 160.103;
18. **"Security Rule"** means the Standards for Security of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164, subparts A and E;
19. **"Secretary"** means the Secretary of the United States Department of Health and Human Services and those employees or agents designated to act on the Secretary's behalf;
20. **"Security"** or "Security Measures" means the administrative, physical, and technical safeguards and documentation requirements specified in the Security Rule; and
21. **"Unsecured PHI"** has the meaning specified in § 17932 of the HITECH Act and 45 C.F.R. 164.402.

Introduction

This Policy explains PAR's practices with respect to the collection and processing of Client ePHI. (For information on how your personal [i.e., Customer] information is handled, please review the general PAR Inc. Privacy Policy at https://www.parinc.com/Privacy-Policy.

Customers can capture and enter Client data (including Client ePHI) and administer and score selected PAR instruments on PARiConnect. If you are a Covered Entity under HIPAA, PAR is your Business Associate with respect to PARiConnect and the confidential ePHI relating to your Clients submitted, stored, or generated via PARiConnect. (You may review the Business Associate Agreement here).

Client data are encrypted on PARiConnect. Although PAR Employees are NOT intended to have access to such data, to ensure full compliance with HIPAA, all PAR Employees who incidentally or accidentally have access to Client ePHI must comply with this Policy.

This Policy further describes:

- PAR's legal obligations with respect to ePHI;
- Mandatory disclosures of ePHI by PAR;
- Permissible disclosures of ePHI by PAR;
- Individual rights; and
- Additional provisions relating to Education Records.

No third-party rights

This Policy is not intended to create any third-party rights, including, without limitation, rights in Clients or other beneficiaries.

Interpretation and scope

To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspiring and shall not be binding. This Policy does not address requirements under other federal laws or under state laws.

Modification

This Policy may be modified or amended from time to time and must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including regulatory changes and modifications). In such an event, the Policy will be revised and made available promptly.

Any changes to this Policy will be effective only with respect to ePHI created or received after the effective date of the Policy, which will be reflected in the "Last Updated" date at the top of the Policy.

General HIPAA privacy policies and practices

Privacy officer and contact person

1. PAR's Privacy and Security Officer is responsible for (a) developing and implementing privacy notices, including this Policy, and privacy procedures including the rules PAR Employees must follow as to any ePHI to which they may be exposed; (b) developing training programs to ensure that all PAR Employees receive the training necessary and

appropriate to permit them to carry out their functions; (c) serving as the point of contact for Customers, Clients, or others with ePHI and other privacy-related questions, concerns, or complaints; and (d) creating a process for individuals to lodge privacy-related complaints and a system for handling such complaints.

2. PAR's Privacy and Security Officer is Travis White. You may contact him at privacyofficer@parinc.com.

Safeguards

1. PAR has implemented appropriate technical, physical, and administrative safeguards to prevent the intentional or unintentional use or disclosure of ePHI on PARiConnect in violation of HIPAA.
2. Technical safeguards include firewalls; strong authentication requirements including unique, secure user IDs and passwords; and encryption of all ePHI.
3. Physical safeguards include locked doors and/or filing cabinets; restricted access to PAR facilities; and implementation of access restrictions and other measures and methods to secure computer workstations, laptops, mobile devices, and other devices and means used to access PARiConnect by PAR Employees.
4. Administrative safeguards include restricting access to ePHI to authorized individuals and limiting access to the minimum ePHI for the relevant assessment administration and/or scoring/interpretation and related functions.

Employee training and sanctions for privacy violations

1. All PAR Employees who may be exposed to ePHI receive training on PAR's privacy procedures and procedures.
2. Any PAR Employee who obtains, uses, or discloses ePHI in violation of this Policy is subject to sanctions up to and including termination pursuant to the disciplinary policy described in the PAR employee handbook (performance improvement section).

Complaints

A copy of PAR's privacy complaint procedure will be provided to any Customer or Client on request.

Mitigation of improper ePHI disclosures

1. On learning that ePHI has been used or disclosed in violation of this Policy, PAR will take steps to mitigate, to the extent possible, any known harmful effects resulting from such use or disclosure.
2. Any PAR Employee who learns of a use or disclosure of ePHI in violation of this Policy by any PAR Employee or outside consultant/contractor is required to immediately notify the Privacy and Security Officer to ensure appropriate and prompt mitigation steps.

Documentation

1. PAR will document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to a Client's privacy rights.
2. The documentation of any policies and procedures, actions, activities, and designations may be maintained in either written or electronic form. PAR will maintain such documentation for at least six years.
3. PAR's HIPAA compliance policies and procedures are also documented and maintained for at least six years, including any changes required to comply with the law (see "Modification" above). All changes to policies or procedures are promptly documented.

Use or disclosure of ePHI

PAR will use and disclose ePHI only as required or permitted under HIPAA and as described below.

Mandatory disclosures (Client or DHHS)

HIPAA requires PAR to disclose ePHI:

1. to the Client who is the subject of the relevant ePHI (see "Access to ePHI, copies, and requests for amendment" below); and
2. to DHHS for purposes of enforcing HIPAA.

Permissive disclosures (legal or policy purposes)

PAR may disclose ePHI without the Client's authorization **only** after satisfying specific requirements (described in PAR's and HIPAA's use and disclosure procedures) **and** obtaining the Privacy and Security Officer's prior approval if the disclosure is:

1. about victims of abuse, neglect, or domestic violence;
2. for judicial and administrative proceedings;
3. for law enforcement purposes;
4. for public health activities;
5. for health oversight activities;
6. about decedents;
7. for cadaver organ, eye, or tissue donation purposes;
8. for certain limited research purposes;
9. to avert a serious threat to health or safety;
10. for specialized government functions; or
11. relates to workers' compensation programs.

Disclosures of ePHI pursuant to an authorization

PAR may disclose ePHI for any purpose if the Client provides an authorization that satisfies all HIPAA's requirements for a valid authorization. All uses and disclosures of ePHI based on a signed authorization must be consistent with the terms and conditions of such authorization.

De-identification/anonymization

The Customer agrees that PAR shall be entitled to de-identify and aggregate data provided to PAR for internal analytical purposes so long as PAR ensures that such data (**"De-identified Aggregated Data"**) are effectively and irreversibly anonymized and de-identified prior to such internal use and that no individual will be identifiable from such data once anonymized and aggregated such that the De-identified Aggregated Data will not constitute "protected health information" or "individually identifiable health information" as defined by 45 C.F.R. §160.103. PAR may use De-identified Aggregated Data internally to improve our products and services. PAR has never and will never deliberately disclose Client ePHI to outside parties.

Individual rights

Access to ePHI, copies, and requests for amendment

1. HIPAA gives Clients the rights (a) to access, (b) to obtain copies, and (c) to request amendment of their ePHI contained by PARiConnect.

2. PAR will provide access to ePHI and consider requests for amendment submitted in writing by Clients and accompanied by appropriate identification verification documents. All such requests must be submitted to the Privacy and Security Officer.
3. PAR will also notify the Customer whose account maintains such Client ePHI of the request for ePHI.

Additional provisions relating to Education Records

It is PAR's policy is to abide by FERPA guidelines, including with respect to Clients who are Students and, where applicable, their parents or legal guardians (**"Parents"**).

Access to Education Records

PAR will assist Educational Agencies or Institutions (collectively referred to as "**Schools**") in providing Parents/Students with an opportunity to inspect education-related reports. Specifically:

1. PAR will comply with requests for information from Schools only;
2. Any such request must pertain to a PAR assessment or test (each an "**Assessment**") taken by a Student;
3. PAR will disclose only the Assessment responses and demographic information;
4. If such material is misplaced or unavailable, the Assessment may have to be retaken for the results to be redistributed. In such cases, FERPA guidelines require this process to be done expediently, and it is the School's responsibility to contact PAR sufficiently in advance to adhere to the 45-day time limit applicable to the School under FERPA (34 CFR § 99.10(b)).

Amendment of Education Records

Parents have the right to request that inaccurate information in an Education Record be changed. Such requests must be directed to the relevant School, which is responsible for confirming the necessity of a correction and communicating the corrected information to PAR. PAR will review requests for correction received only from a School that has confirmed the need for correction and only with respect to information in reports based on Assessments given by PAR Customers. PAR cannot change grades, opinions, or decisions made by the teaching staff of Schools.

Use and disclosure of Student ePHI or Education Records

PAR will use and disclose personally identifiable information relating to Students and submitted, created, generated, and/or stored via PARiConnect only as permitted as to ePHI under HIPAA, or as to Education Records under FERPA, whichever applies.

A Customer may access generated reports by logging into PARiConnect and is responsible for complying with FERPA or HIPAA, as applicable.

If a report is considered part of the Student's Education Record, the Student's Parent (or the Student, if age 18 years or older) seeking access to the report must request the report from the School, which can request the report from PAR. PAR will release a report only to the School and only on receipt of a valid signed consent.

If the School wishes to disclose the report, it must comply with all FERPA requirements for a valid signed consent for disclosure of Education Records (an "**Authorization**") from the Parent or Student, as applicable, and all uses and disclosures made pursuant to an Authorization must be consistent with the terms and conditions of such Authorization.

Under FERPA, Schools may release the report without an Authorization to the following entities or for the following purposes:

- School officials with legitimate educational interest;
- Other schools to which the Student is transferring;
- Specified officials for auditor or evaluation purposes;
- Appropriate parties in connection with financial aid to the Student;
- Organizations conducting certain studies for or on behalf of the School;
- Accrediting organizations;
- Appropriate officials in cases of health and safety emergencies;
- State and local authorities, within a juvenile justice system, pursuant to specific state law; or
- To comply with a judicial order or lawfully issued subpoena.

Previous versions

Previous versions of this PARiConnect Privacy Policy are archived at:
https://www.parinc.com/Legal/PiC-Terms-Archive