

Pearl Inc. Privacy Shield Policies

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law.

Pearl Inc. has chosen to comply with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Frameworks, as applicable, as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and/or Switzerland, as applicable to the United States. Pearl Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles regarding the transfer of personal data from companies in the EU/Switzerland to Pearl.

By adhering to the principles of the Privacy Shield, Pearl agrees to be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) regarding the protection of personal data of private citizens in the EU/Switzerland. The Federal Trade Commission has jurisdiction over Pearl's compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>.

In compliance with the Privacy Shield Principles, Pearl Inc. commits to resolve complaints about our collection or use of your personal information. Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Pearl Inc. at:

ATTN: Chief compliance Officer
Perl Inc.
750 N. San Vicente Blvd.
PDC Red Bldg. #800
West Hollywood, CA 90069
info@hellopearl.com

Pearl Inc. has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) about unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship.

Purpose:

The purpose of this Privacy Policy document is to provide policies and procedures to safeguard and protect the privacy of private personal data. This policy contains Pearl's guidelines and procedures for protecting the security of individually identifiable electronic health information by:

1. Providing a Training to all employees of the Pearl that have access to protected personal data of EU/Swiss patients.

2. Implementing formal documents and controls for the Pearl to protect and safeguard personal data.
3. Training of a compliance officer.

It is the policy of Pearl Inc. to honor a patient's right of access to inspect and obtain a copy of their private personal data; if any, in Pearl's designated record set, for as long as the private personal data is maintained in compliance with Pearl's retention policy.

Procedures for access of data

1. A patient must make a request to a staff member to access and inspect their protected data. Whenever possible, this request shall be made in writing and documented on either the "Authorization for Disclosure" form or in the notes of the patient's health record.
2. Determination of accessibility of the information shall be based on:
 - a. Availability of protected private personal data (i.e., final completion of information, long term storage, retention practices, etc.).
3. Pearl must take action within a reasonable period of time or within 30 days after receipt of the request when the data is on-site, and within 60 days when the data is off-site. One 30-day extension is permitted, if **Pearl** provides the patient with a written statement of the reasons for the delay and the date by which the access request will be processed.
4. Pearl must document and retain the designated record sets subject to access and the titles of persons or offices responsible for receiving and processing requests for access.

Access, Inspection and/or Copy Request is Granted:

1. The patient and Pearl will arrange a mutually convenient time and place for the patient to inspect and/or obtain a copy of the requested data. Inspection and/or copying will be carried out within Pearl with staff assistance.
2. The patient may choose to inspect the data, copy it, or both in the form or format requested. If the data is not readily producible in the requested form or format, Pearl must provide the patient with a readable hard copy form, or other form as agreed to by the Pearl and the patient. If the patient chooses to receive a copy of the data, Pearl may offer to provide copying services. The patient may request that this copy be mailed.
3. Upon prior approval by the patient, Pearl may provide a summary of the requested data.
4. Pearl may charge a reasonable fee for the production of copies or a summary of data if the patient has been informed of such charge and is willing to pay the charge.
5. If, upon inspection of the data, the patient feels it is inaccurate or incomplete, the patient has the right to request an amendment to the data. Pearl shall process requests for amendment as outlined in additional Pearl policy/procedures addressing this patient right.

Access, Inspection, and/or Copy Request is Denied in Whole or in Part

1. Pearl must provide a written denial to the patient. The denial must be in plain language and must contain:

- b. The basis for the denial;
 - c. A statement, if applicable, of the patient's review rights; and
 - d. A description of how the patient may complain to Pearl or to the Secretary of Health and Human Services (HHS).
2. If access is denied because Pearl does not maintain the data that is the subject of the request, and Pearl knows where that data is maintained, Pearl must inform the patient where to direct the request for access.
 3. Pearl must, to the extent possible, give the patient access to any other data requested, after excluding the data as to which Pearl has grounds to deny access.
 4. If access is denied as permitted under §164.524, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by Pearl to act as a reviewing official and who did not participate in the original decision to deny.
 5. The patient must initiate the review of a denial by making a request for review to Pearl. If the patient has requested a review, Pearl must provide or deny access in accordance with the determination of the reviewing professional, who will make the determination within a reasonable period of time.
 6. Pearl must promptly provide written notice to the patient of the determination of the reviewing professional. See paragraph 10 above for denial requirements.

It is the policy of Pearl to honor a patient or a patient's legal representative right to request restrictions on how his or her personal data is used and/or disclosed for the purposes of treatment, payment, and/or healthcare operations and for disclosures permitted under §164.522(a).

Access Requests by Public Authorities:

1. In order to provide transparency in respect of lawful requests by public authorities to access personal information, Privacy Shield organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public authorities for law enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.
2. The information provided by the Privacy Shield organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the annual joint review of the functioning of the Privacy Shield in accordance with the Principles.

Procedures for requesting a restriction of use:

1. Pearl will inform patients of their right to request restrictions on how their personal data is used and/or disclosed for treatment, payment, and healthcare operations in their published, "Notice of Privacy Practices."
2. The patient has the right to request restrictions. Pearl may require the request to be in writing. Pearl's Privacy Officer (or designee) reviews each request and makes a determination of final actions. Effective September 23rd 2013, the American Recovery and Reinvestment Act (ARRA) allows a patient the right to request that a healthcare provider must comply with the patient's request for restriction of disclosure to a health plan for purposes of payment or healthcare operations when the patient health information pertains to a service for which the healthcare provider has been paid in full by the patient "out of pocket."

3. Pearl may agree to a patient's request for restrictions on the use and disclosure of their personal data if the request is determined to be reasonable and, in the patient's, best interests.

When a Request for Restriction(s) Is Accepted:

1. Pearl will notify the patient of the approval of the request.
2. Pearl will inform the patient of any potential consequences of the restriction.
3. Pearl will inform the patient that Pearl will comply with the agreed restriction with the following exceptions:
 - a. In an emergency treatment situation where Pearl may use or disclose information to a health care provider for providing treatment. Pearl will request the emergency treatment provider not further use or disclose the information;
 - b. The restrictions are terminated by either Pearl or the patient; and
 - c. If restrictions prevent uses or disclosures permitted or required under §164.502(a)(2)(ii), §164.510(a) or §164.512.
4. If the agreed upon restriction hampers treatment, Pearl may ask the patient to modify or revoke the restriction. Pearl may require written agreement to the modification/revocation or document the patient's oral agreement.
5. A notice of restriction will be made in writing in the patient's medical record and/or identified in an appropriate field in the computerized patient information system.
6. Pearl will notify separately any other departments to which the restriction may apply (e.g., marketing, public relations, administration, foundation, etc.) and if necessary, ensure that the patient's name is removed from all applicable mailing lists.
7. Pearl will notify separately any other business associates to which the restriction may apply.
8. Pearl will not use or disclose personal data inconsistent with the agreed upon restriction, nor will its business associates, until the restriction is terminated either by Pearl or the individual.
9. Pearl will restrict use and/or disclosure of protected personal data consistent with the status of the restriction in effect on the date it is used or disclosed.

When a Request for Restriction Is Denied:

1. If the request for restriction is denied, Pearl must notify the patient.

Termination:

1. The patient must request in writing to terminate the restriction.
2. If Pearl wants to terminate the agreement, the patient must agree to the termination in writing or an oral agreement must be documented. The termination will be effective with respect to PHI created or received after the patient was notified by Pearl.

Record Retention:

All documentation associated with this procedure will be maintained in writing or in electronic format for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

Arbitration Option:

Any claim, dispute or other matter in question of any kind relating to this Privacy Shield Security Policy which is not resolved by the claims procedures under this Plan shall be settled by arbitration. The arbitration shall be administered by JAMS pursuant to its Streamlined Arbitration Rules. Notice of demand for arbitration shall be made in writing. In no event shall a demand for arbitration be made after the date when the applicable statute of limitations would bar the institution of a legal or equitable proceeding based on such claim, dispute or other matter in question.

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in Section III.11(d)(i) of the Principles; (2) make use of the independent recourse mechanism under the Principles, which is at no cost to the individual; and (3) raise the issue through their Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual. This arbitration option may not be invoked if the individual's same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties.

If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please visit JAMS Cybersecurity and Privacy Practice Group - www.jamsadr.com/cybersecurity, for more information or to file a complaint. The services of JAMS ADR are provided at no cost to you

The decision of the arbitrators shall be final and may be enforced in any court of competent jurisdiction. The arbitrators may award reasonable fees and expenses to the prevailing party in any dispute hereunder and shall award reasonable fees and expenses in the event that the arbitrators find that the losing party.

Notwithstanding the foregoing, upon the mutual agreement of the parties, the parties may submit any such dispute, claim or controversy to non-binding mediation prior to the commencement of arbitration.

Onward Transfers to Third Parties:

The Privacy Shield requires that, "In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf." It is Pearl's policy not to transfer personal information to third parties. The provision regarding liability for the actions of agent processors does not apply because Pearl will not transfer personal information to third parties.