Passport Data Privacy Policy
Version: 3.0

Revision History:

Version	Date	Change Description	Changed By
1.0	2/25/2020	Initial Version	Allen Ampel
2.0	3/31/2021	Annual Review	Allen Ampel
3.0	2/9/2022	Annual review, revised for GDPR	Allen Ampel

1. Policy Statement

It is the policy of Passport Corp ("Company") to use and disclose only the minimum amount of Personally Identifiable Information (PII) and Protected Health Information ("PHI") necessary to accomplish the purpose of the Use or Disclosure. Company must limit requests to HIPAA Covered Entities and Business Associates for PHI to the minimum amount of information necessary to accomplish the purpose of the request.

2. Purpose

This policy and supporting procedures are designed to provide Passport Corp with a documented and formalized Data Privacy policy that is to be adhered to and utilized throughout the organization at all times. Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of Passport Corp's information systems.

This data policy defines the requirements to ensure that information within the organization is protected at an appropriate level and defines the rights and/or processes for PII and ePHI access, portability, erasure, objection, rectification, amendment, restriction, and breach management.

3. Scope

This policy encompasses all information systems that are owned, operated, maintained, and controlled by [Passport Corporation and all other information systems, both internally and externally, that interact with these systems.

- Internal information systems are those owned, operated, maintained, and controlled by Passport Corp and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other information systems deemed in scope.

- External information systems are those owned, operated, maintained, and controlled by any entity other than Passport Corp, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "internal information systems".

- Note: While Passport Corp does not have the ability to actually provision, harden, secure, and deploy another organization's information systems, Passport Corp will follow due-diligence best practices by obtaining all relevant information ensuring that such systems are safe and secure.

This policy applies to the PII and ePHI detailed in the company's **Personally Identifiable Info Matrix** under separate cover.

PASSPORT

4. Policy

All Company Personnel must take reasonable efforts to limit Use, Disclosure of, and requests for PII and PHI to the Minimum Necessary to accomplish the intended purpose of the Use, Disclosure, or request. Disclosures, Uses, and requests must be limited to a Limited Data Set to the extent practicable and comply with any other regulations or guidance defining the Minimum Necessary.

Appropriate Technical and Organizational Measures - At all times, Passport Corp is to implement appropriate technical and organizational measures for ensuring all policy measures are performed with adequate information security controls in place. As such, Passport Corp's initiatives for meeting the required measures for the GDPR – and the stated data protection measures – consists of having formalized, well-documented information security policies, procedures, and processes. Please refer to Passport Corp's Data Protection policy and procedures for more information on the technical and organizational measures in place.

Data Subject Process to Request Action – Data Subjects are allowed to initiate contact with Passport Corp regarding the rights detailed below. Except where otherwise specified below, the following measures are to be undertaken by data subjects should they decide to request action to be taken by the Company:

a. **Complete and return the *Passport Data Subject Action Request* form found at PASSPORTCORP.COM**
b. If your request is valid, we will acknowledge your request in writing and provide you with a reference number relating to your Data Subject Action Request and start processing your records.
c. If your request is valid but we are unable to identify you, we will advise you of this and request additional information.
d. Once Passport Corp has all the required information, your request should be completed within one month. However, if your request is complex, we will take an extension to a maximum of three months and inform you within one month of your request. We also will inform you of the reasons for the delay.
e. If you have sent us an invalid request (e.g., without proof or context), we will return your request along with any enclosures and advise you why your application has been rejected.

Passport Corp is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

f. **ACCESS**
    i. **Regulation Requirements for Right of Access** - Per Article 15 of the GDPR, data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning them is being processed.
    ii. **Procedure for Requesting PII Confirmation from the Company –** see **Data Subject Process to Request Action** section above.
g. **PORTABILITY**
    i. **Regulation Requirements for Right to Portability -** Per Article 20 of the GDPR, data subjects have the right to receive their data in a structured, commonly used and machine-readable format. Additionally, data subjects also have the right to transfer such data without hindrance from the controller. As such, a data subject has the right to transfer their personal data from one controller to another, where technically feasible.
    ii. **Data Subject Right to Portability Measures -** see **Data Subject Process to Request Action** section above.
h. **ERASURE**
    i. **Regulation Requirements for Right to Erasure -** Per Article 17 of the GDPR, data subjects have the right to obtain from the controller the erasure of personal data without undue delay

and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1. Personal data is no longer necessary.
2. Data subject withdraws consent on which processing is based.
3. Data subject objects to processing pursuant to Article 21(1).
4. Personal data has been unlawfully processed.
5. Personal data has to be erased for compliance with a legal obligation with Union or Member State law.
6. Personal data have been collected in relation to services as referred to in Article 8(1).

ii. Data Subject Right to Erasure Measures - see **Data Subject Process to Request Action** section above.

i. **OBJECTION TO ALL PROCESSING**

i. **Regulation Requirements for Right to Object -** Per Article 21 of the GDPR, data subjects have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data, specifically, in relation to Article 6(1), including profiling based on those provisions.

ii. **Data Subject Right to Object Measures -** see **Data Subject Process to Request Action** section above.

j. **RECTIFICATION**

i. Regulation Requirements for Right to Rectification - Per Article 16 of the GDPR, data subjects shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

ii. Data Subject Right to Rectification Measures - see **Data Subject Process to Request Action** section above.

iii. PHI Amendments - An Individual may request that Passport Corp ("Company") amend the Protected Health Information ("PHI") in Company's records pertaining to the Individual, at any time while Company maintains the information. Company will review each request that it receives and make or deny requests as set forth below.

1. Procedures

a. Who May Request. An Individual may request that Company amend or correct PHI in Company's records if the Individual believes the information is inaccurate or incorrect.

b. Form of Request. Requests for amendments or corrections must be made in writing to Company's IT Department. Requests should include the Individual's name, social security number, and an address to which Company should respond with its decision to grant or deny the request. In addition, the request must contain a specific description of information for which the Individual is requesting amendment, the reason for the request, and the contact information of any person or entity with whom Company should share the amendment.

c. Company's Obligations. Company must review and respond to each request for amendment that it receives. Upon receiving a request, Company must act within sixty (60) days to accept, deny, or provide a written statement to extend the time for response to no more than an additional thirty (30) days.

d. Granted Requests. If Company accepts an Individual's request, Company shall notify the Individual in writing that his or her request has been accepted. When Company makes the appropriate amendment, Company must identify all records affected by the amendment and update each of these records.

e. Notice of Amendment. Company must review the Individual's request to identify the relevant persons the Individual has identified to receive notice of the amendment. Company should use reasonable efforts to inform those

persons and any others that Company knows to maintain the information subject to the amendment. Similarly, Company must amend PHI in its possession if it receives this type of notice from a Covered Entity.

f. Denied Requests. If Company denies a request to correct or amend an Individual's PHI, Company must provide the Individual with a statement of the basis for denial, how the Individual may file a written statement of disagreement, and how the Individual may lodge a complaint or statement of disagreement. Company may deny the Individual's request for amendment for any of the following reasons:
    i. Company did not create the information and the originator is available to make the amendment.
    ii. The information is not part of Company's Designated Record Set.
    iii. The information would not be available for inspection, that is, if:
        1. A licensed health care professional has determined that: (i) inspection is reasonably likely to endanger the life or physical safety of the Individual or another person; (ii) the information is about another person and inspection is reasonably likely to cause substantial harm to that person; or (iii) the request is made by the Individual's Personal Representative and Company determines that provision of access to the Personal Representative is likely to cause harm to the Individual or another person.
    iv. The request is to inspect or copy psychotherapy notes.
    v. The request is for information compiled in reasonable anticipation of a legal or administrative action.
    vi. The request is for information maintained by Company that is subject to disclosure limitations under the Clinical Laboratory Improvements Amendments of 1988 ("CLIA").
    vii. Company is acting under the direction of a Correctional Institution and providing access would jeopardize the health, safety, security, custody, or rehabilitation of the Individual or of other inmates, or the safety of any officer, employee, or other person working at or on behalf of the Correctional Institution.
    viii. The request is made during the duration of a research trial and the request is for information created or obtained in the course of research that includes Treatment and the Individual had consented to a denial of access when consenting to participate.
    ix. The request is for information contained in records subject to the federal Privacy Act and denial would be appropriate under that law.
    x. The request is for information that was obtained under a promise of confidentiality and inspection is likely to reveal the source.

g. Future Disclosures when Amendment is Denied. If the Individual submits a statement of disagreement, any future disclosures of the information must include a copy of the Individual's request for amendment, the denial, the statement of disagreement, and Company's rebuttal statement, if any. If the Individual does not submit a statement of disagreement, Company does not have to include this information in future disclosures unless the Individual specifically requests that it do so.

h. Review of a Denial. If Company denies amendment under Section 6(c) (1), the denial is subject to additional review upon request.

k. **RESTRICTION**
    i. **Regulation Requirements for Right to Restriction of Processing -** Per Article 18 of the GDPR, data subjects have the right to restrict processing of their personal data if the following conditions apply:

1. The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
2. The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
3. The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
4. The data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

ii. Data Subject Right to Restriction of Processing Measures - see **Data Subject Process to Request Action** section above.

iii. PHI: It is the policy of Passport Corp ("Company") to recognize and comply with an Individual's right to request restrictions on the Use and Disclosure of the Individual's Protected Health Information ("PHI") beyond the scope of these Policies and Procedures. Company will attempt to honor such requests if, in the sole discretion of Company, the request is reasonable. The Director of IT is charged with responsibility for processing requests for restrictions received from Covered Entity or the Individual. In all cases where Company receives a request for restrictions directly from the Individual, Company will notify Covered Entity of said request. If Company chooses to accept such restrictions, it will be bound to honor them.

1. **Procedures**
    a. Who May Request. An Individual may request a restriction on the Use and Disclosure of PHI either directly from Company or through Covered Entity.
    b. Form of Request. A request for a restriction must be made in writing and submitted to Company's Privacy Officer. Requests should include the Individual's name, social security number, and an address to which Company should respond with its decision to grant or deny the request.
    c. Scope of Restriction. Company will permit Individuals to request restrictions on the Use and Disclosure of their PHI: (a) to carry out Treatment, Payment or Health Care Operations and/or (b) to people involved in their care or for notification purposes as described in § 164.510(b) of the Privacy Regulations. Generally Company is not required to agree to any request to restrict the Use and Disclosure of PHI with one exception. Company must comply with the requested restriction if:
        i. The Disclosure is to a health plan for purposes of carrying out Payment or Health Care Operations (and is not for purposes of carrying out Treatment) except as otherwise required by law; and
        ii. The PHI pertains solely to a health care item or service for which Company has been paid out of pocket in full.
    d. Denial of Restriction. Under certain circumstances, requests for restrictions may be denied. Written notice must be provided informing the Individual of the reasons for the denial. The request for restrictions may be denied if the request relates to:
        i. Psychotherapy Notes.
        ii. information compiled in anticipation of legal or administrative action.
        iii. laboratory results subject to disclosure limitations under CLIA.
        iv. information obtained, under promise of confidentiality, from someone other than a health care provider.
        v. information requested by a parent regarding a minor, if the minor alone sought and consented to the treatment and the treating physician believes it would be in the minor's best interest to maintain the minor's privacy.

vi. information that, in the judgment of a health care professional, (i) could result in possible harm to the Individual or someone else, or another person (other than a health care provider) who might be harmed by the Disclosure; or (iii) is requested by the Individual's Personal Representative but providing access to the Personal Representative could cause harm to the Individual or someone else.
vii. Uses or Disclosure of PHI occurring prior to the date of the request.
viii. Uses or Disclosures that are required by law.

e. Notice of Denial. If the restriction is denied, Company will send the requesting Individual a written notice specifying whether the Individual has the right to appeal the denial. An appeal is allowed only when the denial is based on possible harm, as described in Section 4(f) above.
f. Appeals. Any request for an appeal must be in writing. On receipt of a request, the records in question must be reviewed by a licensed professional who was not involved in the original denial. The review must take place within 30 days of the request for an appeal. If the decision is favorable to the Individual, Company will implement the restriction on the Use and Disclosure of PHI. If the decision is not favorable, Company will notify the Individual in writing immediately.
g. Documentation. Company will retain this version of the policy, together with any forms and other documentation created or obtained in accordance with the policy, for at least six years from the date of last use.

l. **BREACH**
   i. Any breaches will be managed under the ***Passport Incident Response and Breach Reporting Program***

2. Policy Compliance

Compliance Measurement
Management will verify compliance to this policy through various methods, including but not limited to tracking feedback and maintaining records of any reported breach and the resulting actions taken.

Exceptions
None.

Non-Compliance
Employees found to have violated this policy may be subject to disciplinary action, up to and including termination.

Definitions and Terms
Breach means: the unauthorized acquisition, access, Use, or Disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Business Associate:
1. Except as provided in paragraph (2) of this definition, Business Associate means, with respect to a Covered Entity, a person who:

On behalf of such Covered Entity or of an organized health care arrangement in which the Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, performs, or assists in the performance of:

a. A function or activity involving the Use or Disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
b. Any other function or activity regulated by this subchapter; or
 Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the services involves the Disclosure of PHI from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

2. A Covered Entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a services as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a Business Associate of other Covered Entities participating in such organized health care arrangement.

3. A Covered Entity may be a Business Associate of another Covered Entity.

Business Associate Agreement means: A contract entered into by two business partners in which it is agreed to exchange data where the data transmitted is agreed to be protected. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information.

Business Associate Services means: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial services provided by a Business Associate.

Correctional Institution means: any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody.

Covered Entity means: all health care providers, health plans or clearinghouses as defined by HIPAA or any entities which include components engaged in these activities which transmits PHI electronically.

Designated record set means: A group of records maintained by or for Company that includes the medical and billing records about individuals or that are used, in whole or in part, by Company Personnel to make decisions about individuals, regardless of who originally created the information.

1. A Designated Record Set includes, but is not limited to, the following information:
a. Enrollment and eligibility information

b. Payment information

c. Claims adjudication records

d. Case or medical management record systems

e. Any other health information (regardless of whether the information was generated by Covered Entity or was obtained from another health care provider) that either Covered Entity, its third party administrator, or other Business Associates maintain and use to make decisions about providing services to the Individual.

2. A designated record set does not include:
a. duplicate information maintained in other systems;

b. data collected and maintained for research;

c. data collected and maintained for peer review purposes;

d. Psychotherapy Notes;

e. information compiled in reasonable anticipation of litigation or administrative action;

f. health information (regardless of content) provided to and used by Covered Entity for employment purposes;

g. student records; and

h. source data interpreted or summarized in the Individual's medical record (example: pathology slide and diagnostic film).

i. information used or created for Covered Entity's own purposes, such as conducting UR/QA activities, to obtain legal advice, or for other internal operations of Covered Entity.

Disclosure means: any release, transfer, provision of access to, or divulging in any other manner of PHI to persons not employed by or working within Company.

Electronic Health Record or EHR means: An electronic record of health-related information pertaining to an Individual that is created, gathered, managed, and consulted by authorized health care personnel.

Electronic Protected Health Information (ePHI) means: Individually identifiable health information transmitted or maintained in electronic form or medium.

Company means: the named Business Associate herein, Passport Corp ("Company").

Health Care Operations means: Any activity of a Covered Entity protected by HIPAA Regulations including peer review, quality assessment, case management, training, legal and auditing services, fraud investigations, business planning, fund raising, etc. The uses of PHI in operations generally do not require patient authorization.

Health Information means: any information, whether oral or recorded in any form or medium, that:
• Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
• Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Oversight Agency means: An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Record means: a Designated Record Set.

HIPAA means: the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.

HITECH means: The Health Information Technology for Economic and Clinical Health Act which was included in the American Recovery and Reinvestment Act of 2009 ("ARRA") and signed into law on February 17, 2009.

Individual means: the person who is the subject of the PHI.

Law Enforcement Official means: an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set means: A set of data in which most of the Protected Health Information has been removed. The following identifiers of the Individual or of the Individual's relatives, employers or household members must be removed:
• Names
• Addresses, other than town or city, state, and zip code;
• Telephone numbers;
• Fax numbers;
• Electronic mail addresses;
• Social security numbers; 5

• Medical record numbers;
• Health plan beneficiary numbers;
• Account numbers;
• Certificate / license numbers;
• Vehicle identifiers and serial numbers (including license plate numbers);
• Device identifiers and serial numbers;
• Web universal Resource Locators (URLs);
• Internet Protocol (IP) address numbers;
• Biometric identifiers, including finger and voice prints; and
• Full face photographic images and any comparable images.

Marketing means: making a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service.

Minimum Necessary means: the minimum amount of disclosure of PHI necessary to accomplish the purpose underlying the Disclosure.

Personal Representative means: Any person authorized under applicable law to act on behalf of the Individual patient with respect to the Individual's patient's health care.

Psychotherapy Notes means: notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Privacy Rule means: The HIPAA regulations that protect the privacy of health information.

Protected Health Information or PHI means: individually identifiable health information transmitted in any form or medium, including information regarding persons living or deceased. PHI consists of information that is created or received by Company and that relates to: (i) the past, present, or future physical or mental health or condition of an Individual; (ii) the provision of health care to an Individual; or (iii) the past, present, or future payment for the provision of health care to an Individual; and that identifies the Individual or for which there is a reasonable basis to believe the information can be used to identify the Individual.

Research means: a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary means: The Secretary of the Federal Department of Health and Human Services or his/her designee.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. 6

Unsecured Protected Health Information or Unsecured PHI means: Protected Health Information that is not secured through the use of one of the following technologies or methods that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals, or as otherwise further defined or clarified by the Secretary:
a. Encryption: Electronic PHI has been encrypted as specified by the HIPAA Security Rule. See 45 C.F.R. § 164.304 and the regulations related thereto, or in compliance with any guidance issued by the Department of Health and Human Services pursuant to the HITECH Act.
b. Destruction: The media on which PHI is stored or recorded has been destroyed in one of the following ways:
 Paper, film or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

 Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitation, such that PHI cannot be retrieved.

Use means: the sharing, employment, application, utilization, examination, or analysis of PHI by any person working for or within Company.