Global Data Privacy Policy v1.4

Master List Ref	Release Date	Review Date	Next Review Date
PL-ISMS-ENT-012	January, 2017	January, 2023	January, 2024
Version:	**Process Owner**	**Reviewed by**	**Approved by**
1.4	IRM	Shamba Gupta	Sameer Babu

Index:

1. Background:

The purpose of this policy is to explain how Firstsource Solutions Limited's (Henceforth referred to as Firstsource's) business collects, protects, and uses personal data in the endeavor to provide high quality of global services.

Firstsource operates in multiple geographies and recognizes privacy regulations and requirements for the protection of personal data and understands preventing harm to individuals whose data is at stake is crucial to its business.

Firstsource is committed to ensuring that any personal data supplied by its clients, its end customer or otherwise generated by client activities are collected and processed fairly and lawfully.

2. Firstsource Data Privacy Framework

Firstsource has chosen to adhere to the DSCI (Data Security Council of India) recommendations that ensure compliance with the OECD (Organization for Economic Co-operation and Development) privacy guidelines, European Union data protection directives, APEC Privacy framework, Canada PIPEDA (Personal Information Protection and Electronic Documents Act), Australia ANPP (Australia National Privacy Principles), UK Data Protection Act. Firstsource therefore has a detailed privacy policy that addresses the applicable areas out of the following superset defined collectively for the data controllers and processors:

1. Accountability;	2. Notice;	3. Consent
4. Collection limitation	5. Use limitation	6. Disclosures;
7. Access and corrections;	8. Security/safeguards	9. Data quality;
10. Enforcement;	11. Openness;	12. Anonymity;
13. Trans-border data flow	14. Sensitivity	

At a high level the above privacy principles are grouped in the following three areas:

- Principles that advocate user engagement - This pertains to principles such as Notice, Consent and Access and Correction, all of which involve user transactions.;

- Principles that specify how data should be handled - This principle ensures privacy at the data collection stage and mandates requirements such as accuracy, completeness and being up-to-date;

- Principles' demanding security / safeguards and enforcement - This principle specifies the technical, organizational / Process & policy safeguards and liabilities.

3. Applicability of the Privacy principles to Firstsource

Firstsource as a data processor has only the following privacy principles applicable to it:

1. Use limitation;
2. Security;
3. Disclosure to third party;
4. Openness;
5. Accountability.

4. Scope

Firstsource here wishes to distinguish between the "information that it holds or/and processes on behalf of its clients or end customers", data such as Personally Identifiable Data (referred as PII), Protected Healthcare Information (referred as PHI), Payment Card Industry (referred as PCI, Credit card, debit card etc;), and the "corporate information it holds in terms of personal, financial or health information."

This policy applies only to all PII, PCI, or PHI that Firstsource handles as the "data processor". This therefore only applies to Information that it holds or/and processes on behalf of its clients or end customers" and therefore excludes any employee related information that Firstsource holds as an outcome of handling the corporate HR, payroll or any employee engagement program that may exist within Firstsource.

5. Policy

5.1. Use limitation

The use of data and information made available to it by its clients is strictly limited to the sum total of both: the contractual specifications as well as the applicable privacy laws and regulations. In cases of omissions and conflicts, the more restrictive of the two shall prevail as the final requirement.

5.2. Security

Firstsource Information Security team shall formally identify and document the controls that it uses in order to maintain the security of the IUA (Information Usage and Access). Such controls shall include measures and processes that ensure that IUA happens as per the defined client contractual obligations and the applicable data privacy laws for that particular data set;

In accordance with the above principle, Firstsource shall implement and demonstrate controls that meet the following requirements:

a. IRM team shall capture the details of PII, PHI and PCI and other personal / financial data type processed by operations on behalf of its clients and end customer; the document shall capture the details of the controls and concerns for each process in the format F-ISMS-ENT-036 as to the locations of all client PII, PHI or PCI information;

b. The format F-ISMS-ENT-036 shall Document the "Need to" principle – hence ensuring only valid and approved personnel have access to the data;

c. Protection of the boundaries – only data that is required/ or qualifies as "Need to", is being gathered and is accessible to the Firstsource employees;

d. IRM team shall review the format F-ISMS-ENT-036 with business owners on an annual basis to examine and verify that the usage or access is commensurate with the business requirements; the review shall be done over email / phone. The format would be updated with any changes basis the review inputs from business owners;

e. A regular mechanism is in place that looks at the collection, usage and access of all sensitive information that can be used for monitoring the access and usage of all sensitive information on an ongoing basis;

f. The training team shall ensure that all the operations staff / employee processing / handling the personal data such as PII, PHI and PCI for clients / end customer are provided with the data privacy awareness ("GI-ISMS-ENT-036 for IN, UK/NI/ROI, PH, SL", "GI-ISMS-ENT-052" for NA) and its implications at least Annually.

g. Above all, that Firstsource has appropriate controls in place to ensure that all access and storage of sensitive information is in accordance with the guidelines and regulations set forth for PII, PHI and PCI data. This includes controls to be set up for ensuring that personal or financial data such as that of credit or debit cards, health insurance and individual related information are accordingly protected and that prescriptions such as not to store sensitive authentication code(CVV) or pin numbers are enforced.

6. Reporting Privacy Breach

All privacy breach shall get executed every time there is a breach of the above access conditions to centralized support desk.

India / Philippines

Report Breaches / Incidents through the following :

Call CSD (Centralized Support Desk):

- The short dial number : **77777** *(to be dialed in from office)*
- Standard dialing number : **022 61948600 & 022 66983677** *(to be dialed from anywhere outside office)*

- Email: supportdesk.malad@firstsource.com
- Through Intranet – (http://itsm.firstsource.com/SelfService/)

Data Privacy Breach Reporting for North America Healthcare Vertical

Allegations of breaches or concerns relating to disclosures of PHI for North America Healthcare Vertical should be reported to the HIPAA Privacy Officer by calling :

Phone: **1-800-736-2107 ext. 53107**

Email: compliance@na.firstsource.com

To remain anonymous employees can report their concerns to the anonymous reporting hotline by calling **1-877-800-3391.**

Or Log onto the web portal by going to **mai.mycompliancereport.com**

UK

Report violations to ukcompliance@firstsource.com

7. Roles and Responsibility

Roles	Responsibility
1. MISF	• Oversee data privacy policies and their enforcement; • Acceptance and approval authority for highlighted risk post applying the controls and • Oversee reported policy violations and data security investigations; • Advice policy and procedure changes; recommend any additional controls.
2. IRM team	• Review Firstsource data privacy policies to ensure alignment with current practices and regulatory requirements. Oversee data privacy policies and their enforcement within process where PII, PHI and PCI data are processed. • Oversee risk assessments and document identified risks to data in the format F-ISMS-ENT-036 • Oversee reported policy violations and data privacy investigations ;(Exception: Allegations regarding breaches of or other incidents concerning PHI will be investigated by the NA Healthcare Vertical HIPAA Privacy Officer). • Serve as the point person(s) for all external inquiries involving data security compliance issues. • Annually review of data privacy policy and information usage with the respective data processor and business owners. • Review and document security controls for data protection; • Provide Data Privacy awareness training to the identified SPOC (Single Point of Contact) from the respective regions training team.
3. Technology Team	• Implement technology controls as per the Information Security Policy manual (ISMS-001) and Data Privacy Policy (PL-ISMS-ENT-012); • Ensure the technology controls are up to date and ensuring the availability of the controls. • Provides a secure infrastructure in support of the data, including, but not limited to: backup and recovery processes as well as secure transmission and storage of the data • Grant access privileges to authorized data users, documenting those with access, and controlling level of access, ensuring that individuals have access only to that information for which they have been authorized, and that access is removed in a timely fashion when no longer needed (Note: Applicable if data is held within Firstsource Infrastructure and controlled by Firstsource technology team).

4. Data Processor / users	• Employees / data processor / users who are given access to personal , sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of the data • All employees processing and handling PII , PHI , PCI data are responsible for managing the information they collect, create and use as a valuable asset to support only the outcomes of the process and services, • All employees processing and handling PII, PHI, PCI data are responsible for processing the data fairly and lawfully. • All data users shall be aware of the data privacy policies, must have gone through the awareness program and shall be aware of a possible weakness in the protection of data, he or she must report their concerns to the centralized support / report data privacy breaches through their supervisors. Exception: Allegations regarding breaches of or other incidents concerning PHI will be investigated by the NA Healthcare Vertical HIPAA Privacy Officer. • All employees processing and handling PII , PHI , PCI data must ensure the data is not written on paper , printed, Faxed and copied; if it is required for business reason, it must be done only post receiving the authorization and approval from data owners;(Exception for NA healthcare vertical. The use of paper is a standard business practice to process applications, gather documentation for applications, billing of claims via paper, etc. These functions are outlines in the contract so therefore this can be considered 'authorization' from the data owner (client)). All employees processing and handling PII, PHI, PCI data and their supervisors must ensure that any information that is printed / written on paper must be shredded within in the process floor when no longer required. Otherwise it must be stored in secured cabinet (where available).
5. Training Team	• The respective training shall be responsible for cascading the data privacy training to the data users handling PII, PHI and PCI data as per the Data Privacy awareness ("GI-ISMS-ENT-036 for IN, UK/NI/ROI, PH, SL", "GI-ISMS-ENT-052" for NA) annually.
6. Human Resources	• Human Resources shall ensure that the data privacy confidentiality agreement is signed by all the employee and the records of the same is maintained in the employees personal file. • Human resource team shall be responsible to take appropriate disciplinary action for any data privacy breach as per the disciplinary procedure defined by them.

7. Admin & Physical Security	• Admin and physical security team shall ensure that no information written on paper / other material leave the process floor. • Admin team must ensure that appropriate shredder (DoD level 3 and low to medium processing volume) are made available to all the processes where PII (personally Identifiable Information), PHI (protected Health Information) and PCI Data are processed and handled for shredding on the floor.

8. Disclosure to 3rd Party

This shall be in accordance to the laws of land prevailing in the relevant geographies.

Firstsource shall fully cooperate and facilitate monitoring, logging or any other such requirements that the local law enforcement authorities might set.

9. Openness and Accountability

Firstsource shall welcome and cooperate with any checks or audits that might be instituted by clients, end customers, regulatory or advisory bodies, corporate governance requirements and government initiated legal or financial audits.

Annexure A

Information Classification Details

Classification: Firstsource Restricted
Information Owner (IO): Head - Technology
Information Custodian (IC): IRM team
Authorization List (AL): All Employees, 3rd Parties, Existing/Prospective Clients,
Declassify on: Never

Annexure B

Changes since the Last Version (Version)

Date	Version Number	Changes made
24th Jan, 2013	v1.0 to v1.1	1. Section 6 (Reporting Privacy Breach) updated to include additional CSD contact number & e-mail address.
28th Jan, 2014	v1.1 to v1.2	1. Included UK Data Protection Act explicitly under section 2 (Firstsource Data Privacy Framework).
January 4, 2016	v1.2 to v1.3	1. Replaced InfoSec team with IRM team.
January 25, 2017	v1.3 to v1.4	1. Updated the new CSD number in section 6 (Reporting Privacy breach)

Annexure C: Template

1. Template – Data Capture, Visibility of Personal data, and controls and Information Usage.

F-ISMS-ENT-036.xls

2. Template – Data Privacy Confidentiality Agreement.

Data Privacy Policy - Confidentiality Agreer