SECTION 24:

Data Privacy

A. SUMMARY

Carrier respects the legitimate privacy interests of the people from whom it collects, processes, and/or transfers Personal Information, such as its directors, officers, employees, customers, and suppliers. Carrier will take appropriate steps to safeguard Personal Information under its control from unauthorized access, misuse, unauthorized disclosure, alteration, or unauthorized destruction. Personal Information will be disclosed only to Carrier employees, Service Providers, and Third Parties having a legitimate business need to know, as permitted by applicable law, and under appropriate legal and contractual restrictions. Any Carrier Operating Business that is a Covered Entity or a Business Associate will also comply with applicable requirements of the U. S. Health Insurance Portability and Accountability Act and associated regulations ("HIPAA") with respect to Protected Health Information.

B. APPLICABILITY

This Policy applies to Carrier and its Operating Businesses, as defined in Exhibit 1.

Carrier will undertake to have its Service Providers comply with this Policy or equivalent requirements in the conduct of their business with Carrier through appropriate contractual requirements.

Local laws, regulations, and other restrictions applicable to Carrier or any Operating Business shall be applied to the extent of a conflict with this Policy. To ensure that compliance with local laws does not implicate requirements of other jurisdictions, any deviation from this Policy must be approved in writing by the Carrier Data Privacy Counsel ("Carrier Privacy Lead") prior to implementation.

C. DEFINITIONS

Exhibit 1 provides definitions for terms used in this Policy.

All capitalized terms not defined in this Policy (including Exhibit 1) are defined in **CPM 1: Governance and Definitions** including **Exhibit 1: Compliance Glossary**

D. POLICY

1. Compliance with Law: At a minimum, Carrier will comply with all laws and regulations relating to the protection of Personal Information applicable to its Operating Businesses worldwide.

2. Privacy Principles: In all of its activities, Carrier will adhere to the following privacy principles:

    a. Collect and process Personal Information fairly and lawfully;

    b. Identify the purposes for which it is collecting Personal Information and not process the Personal Information for any different purposes unless supported by consent, a legal obligation, a threat of physical harm, or (as permitted by law) a legitimate interest;

    c. Endeavor to ensure that the collection, processing, and transfer of Personal Information is adequate, relevant (the minimum amount needed) and not excessive in relation to the purpose or purposes for which the information is processed;

    d. Make reasonable efforts to confirm that the Personal Information in its possession is accurate and current;

    e. Not keep Personal Information for longer than needed for the purpose(s) for which it was collected, unless otherwise required by law or with consent;

    f. Provide appropriate rights of access, correction, objection, and updating;

    g. Use appropriate technical and organizational measures to prevent unauthorized or unlawful processing of Personal Information and to prevent against accidental loss or destruction of, or damage to, Personal Information;

    h. Not transfer Personal Information from one country to another or from one legal entity to another unless properly supported by law and an adequately secured process;

    i. Provide appropriate written notice to the individuals whose Personal Information it collects, processes, and/or transfers about its practices regarding Personal Information;

    j. Offer appropriate opportunities to opt-out when using Personal Information for direct marketing;

    k. Ensure that an individual is given the chance to discuss the results of any automated decision-making (such as background checks) before any negative action is taken based on that decision-making;

l. Ensure that its handling of employees' Personal Information is consistent with the Employee Privacy Notice, subject to local supplement or amendment to ensure compliance with local law and which shall be accessible to employees and posted on https://carcgl.sharepoint.com/sites/CarrierPrivacy;

m. Only collect Sensitive Personal Information when required by law or for a legitimate business purpose and only as permitted by applicable law, which may require obtaining explicit consent;

n. Take proper care of government-issued identification numbers (such as Social Security Numbers in the U.S. and France, National Numbers in Belgium, Social Insurance Numbers in Canada, Powszechny Elektroniczny System Ewidencji Ludności in Poland, National Registration Identity Card numbers in Singapore, and Resident Registration Numbers in South Korea) by protecting the confidentiality, limiting collection, ensuring access on a need to know basis, implementing appropriate safeguards, including but not limited to encryption, and ensuring proper disposal in accordance with CPM 23: Digital Technology; and

o. Maintain a robust Data Breach Incident Response Plan, respond to and remediate any actual Data Breach Incident, engage the Carrier Communications Team and others, as appropriate, and disclose Data Breach Incidents involving Personal Information, as appropriate and as legally required.

3. **Security**: Carrier will ensure that it maintains reasonable and appropriate technical, physical, and administrative safeguards to protect the Personal Information that it collects, processes, and transfers. These measures will include reasonable restrictions upon physical access to hard copy records containing Personal Information and the storage of such records in locked facilities, storage areas, or containers. Carrier will periodically re-evaluate the measures adopted to ensure that they remain reasonable and appropriate.

4. **Online Privacy**: Carrier will ensure that each of its online websites that collect Personal Information will provide a privacy notice. The privacy notice must identify:

   a. the Personal Information that is to be collected;

   b. the purpose(s) for which that Personal Information is to be collected;

   c. the ways that Carrier will use the Personal Information;

d. “cookies” used by external-facing websites and, if used, how to reconfigure the browser to decline the cookies;

e. third parties with whom Carrier will share the information;

f. the choices provided to individuals, the means for limiting collection, use, and disclosure of Personal Information, and the consequences of those choices; and

g. how to contact Carrier with questions or complaints about privacy matters concerning the website.

Each privacy notice must be reviewed by the owner of the website once every three years to ensure that it is current and accurate. Upon the next review, external-facing Carrier websites that collect Personal Information shall use the template privacy notice contained/referenced in Exhibit 3, with any required modifications, unless permission has been obtained in writing from the assigned Privacy Professional or the Carrier Privacy Lead. Upon the next review, internal-facing Carrier websites that collect Personal Information shall use the template privacy notice contained/referenced in Exhibit 3, with any required modifications, unless permission has been obtained in writing from the assigned Privacy Professional or the Carrier Privacy Lead. Where required by law, Carrier will ensure that Sensitive Personal Information is collected online only with an individual’s explicit consent, via a meaningful opt-in approach, and is appropriately protected against improper use.

5. **Service Providers**: Carrier will enter into a written agreement obligating Service Providers that collect, process, access or possess Personal Information on behalf of Carrier to follow this Policy or equivalent requirements. The written agreement must use the standard terms and conditions, which can be obtained from the assigned Privacy Professional and the Carrier Privacy Lead, who will ensure they are made available on an internal or external website. Modifications must be approved by a Privacy Professional or the applicable Carrier Legal Counsel. The use of Service Providers is also subject to compliance with the IT procedure governing Protection of Carrier Data Entrusted to Third Parties (IT-622).

6. **HIPAA:** Those Carrier Operating Businesses that are subject to HIPAA must:

   a. Maintain reasonable measures to protect the privacy of Protected Health Information;

b. Distribute a notice of privacy practices to the individuals whose Protected Health Information it collects, and post the notice, as required by HIPAA;

c. Enter into Business Associate Agreements with Business Associates of the Operating Businesses and ensure proper and prompt notification of any Data Breach Incident, as addressed in Carrier's Data Breach Incident Response Plan.

d. The Carrier Vice President, Employment & Labor / Compensation & Benefits shall serve as the Carrier HIPAA Privacy Officer; and

e. Comply with other HIPAA-specific requirements set forth in Carrier's policies and procedures.

7. **Transfer Authorization:** Carrier and its Operating Businesses shall rely upon a legal mechanism (such as intercompany agreements or Binding Corporate Rules ("BCRs")) to authorize internal transfers.

   To authorize the transfer of Personal Information to service providers, Carrier and/or its Operating Businesses may enter into the model clauses with a service provider. Where Carrier and/or its Operating Businesses enter into the model clauses, any Carrier entity that is a party to the model clauses shall adhere to them.

8. **Privacy Risk Assessment**: Carrier will implement and maintain an effective privacy risk assessment process to evaluate company-wide risks and appropriate mitigation plans. The Privacy Risk Assessment process will review Carrier's overall collection, processing (including storage and destruction), and transfer of Personal Information and will be updated periodically. The risk assessment also includes the requirement that Carrier and the Operating Businesses conduct a regular privacy self-assessment to assess risk throughout the company.

   To inventory the Personal Information that we collect and use, each Operating Business must ensure that it completes Personal Information Data Inventories at the appropriate level and updates them at a reasonable interval. The Operating Businesses have the flexibility to determine how to implement this requirement so long as it complies with applicable law.

9. **Privacy Impact Assessment:** A written Privacy Impact Assessment must be completed in advance when an Operating Business seeks to: (1) implement a new or modified system or repeating process (such as a survey); (2) use a new or modify the use of a Service Provider; or (3) develop, design, or launch a new or modified technology, product or service – if the system, process, Service

Provider, technology, product, or service will collect, process, or transfer Personal Information. A Privacy Impact Assessment does not need to be completed for: (1) systems or service providers that do not collect, process, or transfer Personal Information; (2) individual actions, such as sending an email or holding a call, but it must be approved for the launch of a new system or service provider or substantial modification of the system or use of the service provider; (3) the new or modified use of a Service Provider that only involves the exchange of Business Contact Information for the limited number of individuals directly working on the transaction(s); and (4) the sale or purchase of hardware or commodities, unless it also involves the provision of a new service or system that tracks Personal Information beyond the Business Contact Information of those involved in the transaction(s). The Privacy Impact Assessment must use the form contained in **OneTrust** or such other form approved by the Carrier Privacy Lead and be reviewed and approved by the Data Protection Officer for the site if there is one, or the designated Privacy Professional, or, if neither is available, the Carrier Privacy Lead. Exhibit 2 contains/references the questions in the Privacy Impact Assessment, but they must be submitted via **OneTrust** (the Exhibit serves as reference only).

10. **Governance**: Carrier will ensure that the Ethics and Compliance Officers understand and are trained to identify privacy concerns, to receive privacy complaints, and to forward both to the appropriate resources for review and resolution. In addition, each Reporting Unit will appoint at least one Privacy Professional to serve as a resource for the Ethics and Compliance Officers and others in the Operating Business with privacy-related issues. The role of the Ethics and Compliance Officers in connection with this Policy and of the Privacy Professional is defined in Section D below. Carrier will ensure that these individuals have sufficient resources and independent authority to perform their role. Carrier will also create and maintain the Privacy Advisory Committee ("Advisory Committee" or "PAC"), which will be responsible for general oversight of Carrier's privacy compliance program. The Advisory Committee will contain representatives from each of the Reporting Units and from Human Resources ("HR"), Digital Technology ("DT"), International Trade Compliance ("ITC"), Environmental, Health & Safety ("EH&S"), Finance, and Supply Management. Other members may be added either temporarily or permanently, as needed.

11. **Training**: Carrier will ensure that Ethics and Compliance Officers, Privacy Professionals, employees who handle Personal Information as an integral part of their responsibilities, and employees involved in the development of systems, tools, services, and/or products used to collect and/or process Personal Information receive annual training on data privacy and security.

12. **Communications:** Carrier will develop and execute a strategic communications plan to raise awareness and educate employees and Service Providers, as appropriate, regarding data privacy and security.

13. **Handling of Complaints and Requests for Access or Correction:** Requests from Individuals regarding the processing of their Personal Information will be addressed as set out below.

a) Internal - From Personnel with access to* Carrier*'s Intranet

Personnel who are direct Carrier employees can address their requests and complaints to their local Human Resources representative. All Personnel, including employees, may contact their Local, Regional, or Global Ethics and Compliance Officer ("ECO"), the Anonymous Reporting Program, or the Privacy Office. These resources can be contacted as follows:

Local HR	Contact using your regular internal channels
ECOs	https://ethics.apps.carrier.com/Pages/ecoRoster.aspx
Anonymous Reporting	**Internet:** https://carrier.webline.saiglobal.com **Telephone:** From within the US & Canada call toll free 855-409-9923. When dialing from outside the USA, you must first dial the AT&T Direct access code for that country, listen for a prompt (voice or tone) and then dial the toll-free number. More information is available at https://corporate.carrier.com/reporting
Privacy Office	privacy@carrier.com

Complaints submitted to local HR, ECOs, or the Privacy Office: these complaints will be addressed by the group (HR, ECO, or Privacy Office) that has received them, with assistance from the appropriate Privacy Professional or the Carrier Privacy Lead (or designee) where needed.

Privacy complaints submitted to the Anonymous Reporting Program: so long as the complainant seeks a further response and agrees, those complaints will be forwarded to the Privacy Office for response and resolution.

b) External - From all other Individuals

Requests and complaints from all other Individuals can be addressed to the Anonymous Reporting Program or the Privacy Office, which can be reached as follows:

Anonymous Reporting	**Internet:** https://carrier.webline.saiglobal.com **Telephone:** From within the US & Canada call toll free 855-409-9923. When dialing from outside the USA, you must first dial the AT&T Direct access code for that country, listen for a prompt (voice or tone) and then dial the toll-free number. More information is available at https://corporate.carrier.com/reporting
Privacy Office	privacy @carrier.com

So long as the complainant seeks a further response and agrees, privacy complaints submitted to the Anonymous Reporting Program will be forwarded to the Privacy Office for response and resolution.

c) Additional information about complaint handling

Complaints and audit results revealing structural shortcomings globally will be addressed by the Carrier Privacy Lead through the Privacy Advisory Committee.

Any time a complaint cannot be resolved to the complainant's satisfaction, local HR, the ECO, or the Privacy Professional will report the issue to the Carrier Privacy Lead.

Carrier will endeavor to provide an initial response within five working days of receiving the request/complaint. Depending on the complexity and scope of the request/complaint, this period may be longer, but should not exceed one month.

14. **Monitor and Audit:** The Carrier Vice President, Ethics & Compliance and the Carrier Director, Internal Audit, will administer assurance and audit programs to evaluate compliance with this Policy by staff organizations and Operating Businesses. The audit program will cover compliance with this policy, including the BCRs. Results of audits covering BCRs will be communicated to the Carrier Privacy Lead, who, in turn, will inform the Carrier Vice President, Ethics & Compliance, and the Privacy Advisory Committee.

15. **Enforcement**: Carrier will enforce this Policy and the procedures issued to implement it. Failure to adhere to this Policy or the procedures implementing it may lead to disciplinary action for employees. Carrier will establish clear, fair, and consistent disciplinary procedures across the enterprise.

E. RESPONSIBILITIES

1. Carrier **employees and leased labor** (e.g., onsite contract workers) must comply with this Policy and all procedures issued to implement it. All employees and leased labor must safeguard Personal Information and report any known or suspected Data Breach Incident immediately as directed in the Data Breach Incident Response Plan, which is part of CPM 10, § 2: Data Protection.

2. **The Vice President, Chief Information Security Officer** (CISO) shall be responsible for maintaining, monitoring, and improving, as needed, reasonable and appropriate technical, physical, and administrative safeguards to protect the Personal Information that Carrier collects, processes, and transfers through information technology assets and systems. The CISO will ensure that the DT organization receives training on this Policy, provides information and consultation about where data is stored, processed, and transferred, and actively works to ensure integration of the requirements of this Policy in the design, implementation, maintenance, and use of Carrier DT systems and assets. The CISO will ensure that the Carrier Privacy Lead, is informed with respect to procedures for data security and Data Breach Incident response. The CISO must also identify a person to serve on the Advisory Committee to represent Digital.

3. **The Carrier Senior Vice President Chief Human Resources Officer** (CHRO) shall be responsible for implementing procedures to ensure that all Personal Information collected, processed, and transferred by HR shall be done consistent with this Policy. The CHRO shall also identify a member of the Privacy Advisory Committee to represent HR. The CHRO will ensure that local HR participates in annual training and understands their role in promoting compliance with this Policy.

4. **The Presidents of each Reporting Unit** will establish and maintain a privacy compliance program that is consistent with this Policy. The Presidents will retain general oversight and management responsibility for the privacy compliance program and the effective function of the people implementing it for their organization. The Presidents will ensure that each Reporting Unit has at least one person who can serve as a Privacy Professional, who can provide guidance on this Policy and its requirements. The Privacy Professional may serve in a full-time or part-time capacity and may sit in Legal, HR, DT, or Ethics and Compliance. Each Privacy Professional must participate in privacy-related annual training provided by Carrier and must participate in at least one external conference or seminar every two years. Each Privacy Professional must also serve on the Advisory Committee. The Presidents will ensure that the identity of the Privacy Professionals is communicated adequately throughout the business.

5. **The General Counsels of each Reporting Unit** will ensure that their legal department is trained on, and provides assistance in, drafting and negotiating required agreements implementing this Policy, including data transfer agreements required to support cross-border transfers of Personal Information.

6. **The Carrier Leads for ITC, EH&S, Finance and Supply Management** must ensure that their function complies with this Policy, appoint a person to serve on the Advisory Committee for their organization, and ensure that individuals in their function identified as handling Personal Information as an integral element of their jobs receive annual training on this Policy.

7. **Ethics and Compliance Officers** (ECOs) will facilitate compliance with this Policy and be the point of contact for comments and complaints relating to this Policy. ECOs must be knowledgeable about resources available in Carrier to address privacy issues. ECOs must participate in annual training.

8. **Data Protection Officers** will be appointed where required by applicable law. The role of the Data Protection Officer will be defined by applicable law.

9. **Privacy Professionals** will be responsible for providing guidance on the implementation of this Policy and understanding and researching applicable local laws to ensure that any additional legal requirements are met. For any site where there is no Data Protection Officer, Privacy Professionals are responsible for reviewing and approving where appropriate the Privacy Impact Assessment forms submitted from their assigned Operating Businesses. Privacy Professionals must attend an external conference on privacy/data protection at least once every two years and must participate in Carrier training on this Policy.

10. **The Privacy Advisory Committee** will identify data privacy and security issues that require resolution and will advise the Carrier Privacy Lead on the deployment and improvement of this Policy as well as the procedures promulgated to implement it to ensure that the Policy and the procedures are effective and efficient.

11. Carrier **Internal Audit** will audit the Operating Businesses and functions to ensure compliance with this Policy.

12. **The Carrier Privacy Lead** will deploy this Policy and ensure that it is effectively and efficiently implemented. The Carrier Privacy Lead will also be responsible for training and awareness campaigns on data privacy and for supporting the Privacy Professionals and ensuring that they are trained, while promoting the existence and purpose of data privacy requirements in addition to basic requirements for the protection of proprietary information. The Carrier Privacy Lead will maintain the Online Privacy Notice template (Exhibit 3) and Service Provider data privacy terms and conditions templates and review exceptions to

those templates. The Carrier Privacy Lead must consult with DT on Data Breach Incidents and IT Security as it pertains to Personal Information.

13. **The Carrier Vice President, Ethics & Compliance** will oversee promulgation and implementation of this Policy and the program deployed to implement it.

14. **The Privacy Office** consists of the Carrier Privacy Lead, the Privacy Professionals, and any appointed Data Protection Officers, as well as any additional personnel appointed by the Reporting Units or the Corporate Office. The Privacy Office participates on the PAC, responds to and resolves any comments or complaints that come into the Privacy Office or through the Carrier Anonymous Reporting Program, and assists the ECOs in responding to and resolving any comments or complaints that are submitted to the ECO team.

F. REFERENCES

Carrier Code of Ethics

CPM 10: Intellectual Property

CPM 23: Digital Technology

CPM 14: Corporate Governance & Records

Carrier HIPAA Privacy Notice

Carrier Employee Privacy Notice

G. REVIEW

This Policy will be reviewed by the Carrier Privacy Lead at 2-year intervals following its issuance, and more often as dictated by changing legal requirements. Carrier will notify employees of any material changes and publish pertinent updates to required notices.

EXHIBIT 1

Definitions

"Business Associate" is a person or entity that performs certain functions or services for or on behalf of an Operating Business that is a Covered Entity, where the functions or services involve the creation, receipt, maintenance, or transmission of Protected Health Information. The term includes, for example, service providers that create, receive, maintain or transmit Protected Health Information for purposes of assisting with health insurance or disability claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or providers of legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services where the provision of the service involves the disclosure of Protected Health Information. The U.S. Health Insurance Portability and Accountability Act ("HIPAA") defines a Business Associate in 45 C.F.R. § 160.103 (and that definition controls to the extent that it conflicts with this one). A person or entity (including an Operating Business) that is a subcontractor of a Business Associate is also defined as a Business Associate under HIPAA if the subcontractor performs functions or services for or on behalf of the Business Associate that involve the creation, receipt, maintenance, or transmission of Protected Health Information.

"Business Contact Information" includes the name, business telephone, business address, and business email for an individual when used in the person's work capacity. In many countries, Business Contact Information is protected and this Policy treats it as Personal Information.

"Covered Entity" is a health insurance plan, health insurance clearinghouse, or health care provider that transmits certain information (such as claims or payment) electronically. HIPAA only applies to entities operating in the United States. Carrier and its subsidiaries and affiliates are Covered Entities if they self-insure or provide health care services for which claim, payment, or referral information is sent electronically. The U.S. Health Insurance Portability and Accountability Act ("HIPAA") defines a Covered Entity in 45 C.F.R. § 160.103 (and that definition controls to the extent that it conflicts with this one).

"Data Breach Incident" is defined in § 2: Data Protection of CPM 10: Intellectual Property.

"**OneTrust**" is the online tool used for submitting Privacy Impact Assessments, the regular Privacy Self-Assessment, and the Personal Information Data Inventory.

"Operating Businesses" means Carrier's business segments, units and divisions, and all other operating entities wherever located (including controlled joint ventures, partnerships and other business arrangements where Carrier has either a controlling interest or effective management control), other than the Carrier Corporate Office.

"Personal Information" means information relating to an identified or identifiable natural person. This is any information relating to a natural person, identified or identifiable, directly or indirectly, in particular by reference to an identifier, such as an identification number, name or one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identity. Whether an individual is identifiable depends on the means reasonably likely to be used by Carrier or another person to identify the individual concerned. Where these measures are not reasonably likely to be used or identification is impossible, the data concerned are anonymous and not covered by CPM 24. The term includes Sensitive Personal Information. Personal Information includes information collected, processed, and/or transferred regardless of the medium, including but not limited to hard copy, electronic, video recording, and audio recording.

"Protected Health Information" or "PHI" is a term unique to HIPAA and means all Individually Identifiable Health Information held or transmitted by a Covered Entity, in any form or media, whether electronic, paper, or oral. "Individually Identifiable Health Information" is information, including demographic data, that relates to an individual's past, present or future physical or mental health or condition; the provision of healthcare to the individual; or the past, present, or future payment for the provision of healthcare to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually Identifiable Health Information includes many common identifiers (e.g., name, address, birth date, Social Security number, etc.).

"Sensitive Personal Information" is a subset of Personal Information and means information relating to an identified or identifiable person that involves: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sexual preference; sex life; or the commission or alleged commission of any crime and possible penalties.

"Service Provider" means any entity or person who processes or is otherwise permitted access to Personal Information processed by Carrier through its provision of services directly to Carrier.

"Third Party" is any individual or entity, other than Operating Businesses and their employees, and Service Providers.

EXHIBIT 2

Privacy Impact Assessment

The questions included in the current Carrier Privacy Impact Assessment are accessible under the following URL: https://app.onetrust.com/ (login required).

EXHIBIT 3

Privacy Notices

Carrier maintains the following Privacy Notices:

- General Privacy Notice
- Online Privacy Notice for External-Facing Websites (Landing Page Privacy Notice)
- Online Privacy Notice for Internal-Facing Websites and Workflows
- Employee Privacy Notice
- HIPAA Privacy Notice
- Job Applicant Privacy Notice

These Privacy Notices are accessible via the Privacy SharePoint under the following URL: **https://carcgl.sharepoint.com/sites/CarrierPrivacy**