U.S. PRIVACY STATEMENT

Last updated: December 31, 2022

Content

1	Introduction	2
2	When does this Privacy Statement apply?	2
3	What Personal Information do we collect and process?	2
4	How do we collect your Personal Information?	4
5	For which purposes do we collect and process your Personal Information?	4
6	Do we use cookies?	5
7	How do we handle and secure your Personal Information?	6
8	Do we transfer your Personal Information to third parties and / or to other countries?	6
9	What additional privacy rights are offered to residents of California or Nevada or minors?	7
10	How to contact us in case of a request, complaint, or question?	10
11	Privacy statements and other consumer privacy notices	11

1 Introduction

Philips Medical Capital, LLC (“PMC”, “we,”, “us”, or “our”), provides innovative financing solutions tailored for the healthcare community. PMC collects and processes Personal Information relating to individuals, including but not limited to our customers, suppliers, business partners, employees, contractors, and job applicants. Personal Information means information that identifies, relates to, could reasonably be associated or linked, directly or indirectly, with you or your household. The privacy and the protection of Personal Information is important to PMC. This Privacy Statement provides information on how PMC may collect and process your Personal Information.

This Privacy Statement can change over time. The changes we made to the Privacy Statement will become effective upon posting as of the Last Updated Date as shown above. This is the most up-to-date version. The most recent previous version of our Privacy Statement can be found at the bottom of this Privacy Statement.

By accessing or using the Services (as defined in Section 2), you consent to this Privacy Statement. If you have any objection to any terms in this Privacy Statement, please reach out to us as instructed in Section 10 below.

PMC is a joint venture co-owned by ultimately, DLL U.S. Holdings Company, Inc., (“DLL”) and Philips North America LLC. DLL is a wholly owned subsidiary of Coöperatieve Rabobank U.A. (‘Rabobank’ and together with its subsidiaries, the ‘Rabobank Group’). Entities within the Rabobank Group will be deemed an “Affiliate” of PMC.

2 When does this Privacy Statement apply?

This Privacy Statement applies to the collecting and processing (including storing, accessing, using, transferring, disclosing, and deleting) of Personal Information by PMC of:

- Visitors and users of PMC websites;
- Users of PMC’s services, products, and/or tools (“Services”);
- Customers and prospective customers and their respective representatives;
- Business partners of PMC and their representatives;
- Suppliers who provide any services or products to PMC and their representatives;
- Employees and contractors of PMC;
- Job applicants to PMC’s employment positions;
- Subscribers to PMC publications and newsletters;
- Visitors to PMC offices and facilities; and
- Individuals who otherwise interact with PMC in person, in writing, or through a third party.

This Privacy Statement does not apply to information you provide on third party sites not controlled by PMC. When interacting with our websites, you may be able to link or connect with non-PMC websites, services, social media networks, applications, or other third-party features. Enabling these features may lead to other third parties having access to or processing your Personal Information. PMC does not have any control over, nor do we endorse, these third-party features and is not responsible for the privacy or security of any information you provide to any such third-party website. We encourage you to review the privacy policies of these third parties before using these features.

3 What Personal Information do we collect and process?

PMC collects and processes Personal Information in a variety of contexts. For example, we collect and process Personal Information to provide individual and commercial financial products and services, and for employment and human resource purposes, as applicable.

a) The Personal Information, including Sensitive Personal Information (as defined in Section 9), we collect and process depends on your relationship or interaction with PMC. We collect and process the following categories of Personal Information:

   1. Personal Identifiers and Contact Information—such as business name, full name, address, telephone number, and federal or state issued identification numbers, including Social Security number, driver's license number, and passport number, Internet Protocol address information, email address, or account name.

   2. Characteristics of Protected Classes--under federal or state law, such as gender, race, ethnicity, national origin, citizenship, marital status, or military status.

   3. Purchase and Financial Information—such as information about your financial situation, information related to our products or services, information related to obtaining financial services, bank account information, or your credit risk profile.

   4. Internet or Online Information— such as IP address, data about the applications and devices you use to visit our website, browsing and search history, interaction with our websites, applications, advertisements, user login and access information, or language preference in the context of using our services.

   5. Geolocation Data—such as device or equipment location.

   6. Audio, Visual, and Electronic Information—such as call, online chat, email, or video recordings.

   7. Inferences—inferences based on information about an individual to create a summary about, for example, an individual's preferences and characteristics.

   8. Professional or Employment Information—such as business entity information, professional affiliations, or work history.

b) If you are a customer, dealer, vendor, supplier, or other business partner of PMC, in addition to the Personal Information listed above, we also collect and process the following Personal Information:

   1. Background Information—such as data we require to ensure your and our security, to prevent and investigate fraud, to prevent money laundering and financing of terrorism.

   2. Information about commercial or consumer needs--such as business needs and operational information, records of personal property, products or services purchased, obtained, or considered, payment history, or other purchasing or consuming histories or tendencies.

c) If you are an employee, contractor, or job applicant, in addition to the Personal Information listed above, we also collect and process the following Personal Information, including Sensitive Personal Information, as applicable:

   1. Family Information—such as name(s) and contact information of your partners, children, or other family members.

   2. Background screening—such as criminal and financial background checks.

3. Educational Information—such as school, professional training and qualification, and related information.

4. Financial, Health, and Benefits Information—such as compensation, payroll data, tax information, bank account information, health, dental, and vision claims and/or information, disability and life insurance claims, unemployment, or retirement account information.

5. PMC Specific Employment Information—such as screening, job title, office location, business activities, performance evaluation, or work-related contacts and communications.

6. Vehicle and Driving Information—such as information about your use of business leased cars and your personal vehicle's information when parked in a PMC office parking lot.

7. Biometric Information—such as fingerprints, voiceprints, video recordings, or photos.

8. Information required to fulfill legal obligations—such as child support obligations, worker's compensation, unemployment, and other similar information.

From time to time, laws and regulations may require us to collect additional categories of Personal Information from you.

4 How do we collect your Personal Information?

The sources from which we collect Personal Information depend on, among other things, our relationship or interaction with you. The information below lists the categories of sources from which we collect Personal Information in different contexts.

1. You directly, or other authorized parties acting on your behalf, through physical (e.g., paper application, visitor registration when you visit our office), audio (e.g., phone), visual (e.g., Closed Circuit Television monitoring when you visit our offices), or electronic (e.g., website, social media) sources.

2. Public records made available by federal, state, or local government entities or widely available sources made available by media.

3. Third parties that provide data to support our business and operational activities, human resources and workforce management activities, such as our Affiliates, joint venture partners, business partners, manufacturer, vendors, dealers, distributors of goods or service you finance with us, credit bureaus, employee benefit providers, and suppliers who provide goods and services to us.

4. Equipment you finance with us.

5 For which purposes do we collect and process your Personal Information?

The purposes for which we collect and use Personal Information depend on, among other things, your relationship or interaction with PMC. We collect and process Personal Information for the following purposes in different contexts:

Purposes of Collection and Process	Examples
Enter into, fulfill, maintain, and service a contract with you or otherwise provide Services to you	• Establish and process transactions for our Services. • Process financial applications, assess your eligibility for our products and services, and verify your identity. • Perform integrity screening and credit checks. • Maintain and service your accounts and provide customer service. • Process payments.
Promotion and marketing	• Advertise and market additional products and services that are related to Services you requested or that are offered by us, or Affiliates, or a nonaffiliated third party. • Administer promotions, surveys, pools, sweepstakes, and contests.
Support business operations, including to meet risk, legal, and compliance requirements	• Conduct audits and compliance assessments. • Facilitate securitizations, syndications, or loan or lease participations. • Facilitate sale, transfer, merger, reorganization, or other change to a business line or legal entity/structure. • Detect, investigate, or respond to legal claims, security incidents and malicious, deceptive, fraudulent, or illegal activity. • Comply with applicable local, state, federal, and international laws and other legal and regulatory requests and obligations. • Process privacy rights requests. • Maintain safety, security, and integrity of our offices and Services.
Manage, improve, and develop our business and Services	• Conduct internal research, product quality, risk modeling, data analysis, internal presentation. • Troubleshoot to identify and repair operational errors or otherwise improve our Services.
Support employment, human resources, and operational management	• Provide employment benefits and other employment-related services to employees and dependents. • Manage payroll and compensation activities. • Process employment applications. • Manage and operate our facilities and infrastructure.

6 Do we use cookies?

When you visit our website or use our applications, we may automatically collect information about how you use our Services using cookies, pixel tags, web beacons, and other similar or related technologies. Some of this information is not capable of identifying you but some information can be associated with you, your browser, or your device. We have relationships with third-party advertising companies to help track and report on usage of our website and applications.

Various third parties are developing or have developed signals or other mechanisms for the expression of consumer choice regarding the collection of information about an individual consumer's online activities over time and across third-party websites or online services.

Currently, we currently do not monitor or take any action with respect to your “do not track” preferences.

7 How do we handle and secure your Personal Information?

We endeavor to protect your Personal Information. To prevent unauthorized access, disclosure, or use of your Personal Information, we have implemented and maintain appropriate and reasonable technical and organizational security measures to safeguard and secure your Personal Information. We use security measures designed to ensure (i) the confidentiality, integrity, and availability of your Personal Information, (ii) the resilience of the systems and services that process them, and (iii) the ability to restore data in the event of a data breach. Where possible, we aim to secure your Personal Information using encryption measures. In addition, we test, verify, and regularly evaluate the effectiveness of our technical and organizational measures to ensure continuous improvement in the security of processing Personal Information.

8 Do we transfer your Personal Information to third parties and / or to other countries?

a. Within the Rabobank Group

Your Personal Information may be disclosed on a confidential basis within the Rabobank Group for the purposes described in this Privacy Statement, to the extent permitted by applicable law and in accordance with the Rabobank Group’s internal policies.

b. Outside the Rabobank Group

In certain instances, your Personal Information may also be transferred to third parties outside the Rabobank Group. The categories of third parties to whom we may disclose your Personal Information depend on, among other things, our relationship and/or interaction(s) with you. We may disclose for our business purposes the categories of Personal Information listed in Section 3 above to the following categories of third parties:

1. **Business Partners and Service Providers:** We may disclose your Personal Information to third-party companies or organizations to complete transactions, support everyday operations, or for our business management and development purposes. Examples include disclosing to our manufacturers, vendors, dealers, distributors, business partners, credit bureaus, employee benefit providers, service suppliers, and other third parties, all as may be necessary for us to provide our products and services to you.

2. **Advertisers and/or Marketing Agencies:** Where permitted by applicable law and/or with your consent, we may disclose your Personal Information to third party advertisers or marketing agencies that process your Personal Information on our behalf for marketing purposes. The privacy policy of such third-party advertisers or marketing agencies will govern their use of your Personal Information.

3. **Legal and Regulatory Obligations:** We may also disclose your Personal Information to third parties when necessary to (a) enforce or apply the terms and conditions of the Services, including in connection with an investigation of potential violations of any such terms and conditions, (b) comply with legal or regulatory requirements or a governmental request or inquiry, (c) protect the rights, property, or safety of us, our customers, or other third parties, (d) prevent, investigate, detect, or prosecute a crime or protect national security, or (e) detect, prevent, or otherwise address fraud, security, or technical issues.

4. **Business Transaction or Reorganization:** We may also transfer your Personal Information to a third party in the event of a sale, merger, or transfer of our company's equity or assets or in the unlikely event of a bankruptcy, liquidation, or receivership of our business.

Lastly, we reserve the right to disclose anonymized or aggregated data based on your Personal Information to third parties, provided that such information can no longer reasonably identify or be linked to you or your household.

Cross-Border Transfers of Collected Personal Information

PMC transacts business in multiple locations throughout the U.S. and around the globe, and has Affiliates located in various countries throughout the world. Your Personal Information may be accessed, processed, or transferred to Affiliates and other third parties in the U.S. and elsewhere in the world for the purposes described in this Privacy Statement to the extent permitted by applicable laws.

9 What additional privacy rights are offered to residents of California or Nevada or minors?

Depending on your state of residency or age, and subject to certain legal limitations and exceptions, you may have additional privacy rights with respect to your Personal Information.

Residents of California:

If you reside in the state of California, the additional privacy notice set forth in this section is applicable to you pursuant to the California Consumer Privacy Act, as amended by the California Privacy Rights Act and its implementing regulations (collectively, the "CPRA").

Collection, Use, and Disclosure of Personal Information

In the past 12 months, we have (i) collected from sources listed in Section 4, the categories of Personal Information and Sensitive Personal information from you that are listed in Section 3; (ii) used, disclosed, or processed such Personal Information for the purposes provided in Section 5; and (iii) disclosed the categories of Personal Information listed in Section 3 with the categories of third parties that are listed in Section 8. Sensitive Personal Information under CPRA means a class of protected Personal Information, including: Social Security numbers, driver's license numbers, passport numbers, account log-in names and passwords, geolocation data, racial or ethnic origin data, religious or philosophical belief data, union membership data, the contents of mail, email or a text message, genetic data, the processing of biometric information for the purpose of identifying an individual, and data regarding sexual orientation or preference.

PMC may use, process, or disclose your Sensitive Personal Information we collect for one or more of the following purposes:

- To perform or provide the Services reasonably expected by you;
- To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, and/or confidentiality of Personal Information;
- To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions;
- To ensure the physical safety of natural persons;

- For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of your current interaction with PMC;
- For third parties to perform Services on behalf of PMC;
- To verify or maintain the quality or safety of Services or devices that are owned or controlled by PMC, and to improve, upgrade, or enhance the Services or devices that are owned or controlled by PMC;
- To collect or process Sensitive Personal Information where such collection or processing is not for the purpose of inferring characteristics about you;
- For any other acceptable purposes as set forth in the CPRA.

PMC may disclose Personal Information, in some cases Sensitive Personal Information, to our "service providers", to our "contractors", and to "third parties" (each as defined by the CPRA) for a business purpose. When we disclose Personal Information for a business purpose, we endeavor to enter into an agreement with the receiving party that describes the purpose for disclosing the Personal Information and requires the receiving party to keep that Personal Information confidential and to comply with applicable laws.

In the past 12 months, we have not "sold" or "shared", as such terms are defined under the CPRA, your Personal Information.

Retention of Personal Information

We endeavor to retain each category of your Personal Information for no longer than what is reasonably necessary for one or more business purposes according to our internal retention policy. We use the following criteria to determine the applicable retention period(s):

- whether there is a retention period required by applicable laws or regulations;
- pendency of any actual or threatened litigation for which we are required to preserve the information;
- pendency of applicable statutes of limitations for potential legal claims; and
- business needs or generally accepted best practices in our industry

When we determine that it is no longer reasonably necessary to retain your Personal Information for one or more disclosed business purpose(s) based on the above criteria, we will endeavor to delete or de-identify your Personal Information or, if this is not possible (for example, because Personal Information has been stored in backup archives), then we will securely store your Personal Information and isolate it from further processing until deletion or deidentification is possible.

Your Rights and Choices:

1. **Right to Know and Portability**: you may request that we disclose to you the following information covering the 12-month period prior to your request if you submit a Verifiable Request (as defined in Section 10, below) (such request, an "Access Request"):
    a. The categories of Personal Information collected about you.
    b. The categories of sources from which your Personal Information was collected.
    c. The purpose for collecting or disclosing your Personal Information.
    d. The categories of third parties to whom Personal Information is disclosed about you, and the categories of Personal Information disclosed.
    e. The specific pieces of Personal Information collected about you.

f. If we disclosed your Personal Information for a business purpose, what categories of Personal Information we disclosed for a business purpose, and to which categories of recipients we disclosed it to.
g. You may request a copy of your Personal Information, and/or request that we transmit your Personal Information to another entity. To the extent technically feasible, we will comply with your request and provide and/or transmit your Personal Information in a structured, commonly used, and machine-readable format.

2. **Right to Delete**: you may request that we delete certain Personal Information collected about you by submitting a Verifiable Request ("Deletion Request"). We may deny your Deletion Request if retaining your Personal Information is necessary for us or our service providers to:

    a. Complete the transaction for which we collected your Personal Information, provide goods or services that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you;
    b. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
    c. Debug products to identify and repair errors that impair existing intended functionality;
    d. Enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us;
    e. Make other internal and lawful uses of that information that are compatible with the context in which you provided it; and
    f. Comply with legal obligations, laws, and regulations, including other denial grounds provided under CPRA.

3. **Right to Correct**. You have the right to request that we correct any of your Personal Information that is inaccurate by submitting a Verifiable Request. We will correct any inaccurate Personal Information pursuant to your request to the extent possible using commercially reasonable efforts. We may deny your correction request if the Personal Information is accurate.

4. **Right Not to Receive Discriminatory Treatment**: You have the right to be free from discrimination by PMC for exercising your rights under the CPRA.

After we receive your Verifiable Request, we will provide to you, in writing and free of charge (unless your request is excessive, repetitive, or manifestly unfounded), the requested information for the 12-month period preceding your request. If you specifically request disclosure beyond such 12-month period, we will process your request with respect to Personal Information we have collected during the time-period you specify, provided that (a) the earliest date that your request may apply to is January 1, 2022, and (b) processing your request does not require disproportionate effort. We will try to respond to your Verifiable Request within forty-five (45) days of receipt, but if we require more time (up to another forty-five (45) days), we will inform you of the reason and extension period in writing. Please note that we are not required to comply with your request for information more than twice in any 12-month period. If applicable, our response will explain the reasons why we cannot comply with your request. We may deny your request if it is fraudulent, excessive, repetitive, harassing, or manifestly unfounded.

Authorized Agents

If you are a California resident, you may authorize an agent to make a request on your behalf in accordance with the "How to Make Requests" instructions in Section 10 below.

Residents of Nevada

Nevada's data privacy law defines selling Personal Information as exchanging it for money. We do not sell Personal Information of residents of Nevada. However, you may contact us at usprivacyoffice@philipsmedicalcapital.com with questions.

Notice to Minors

Our customer-facing websites are not designed for minors and are not directed at or intended to be visited by minors. No visitor to our websites who is under the age of eighteen (18) should provide any Personal Information to us. If you are a minor, do not visit our websites and do not send any Personal Information to us.

If we become aware that we have collected Personal Information from a minor, we will take steps to delete such information in accordance with applicable laws and regulations. If you are a parent or guardian and you believe that your child under the age of eighteen (18) has provided us with Personal Information without your consent, please contact us at usprivacyoffice@philipsmedicalcapital.com.

10 How to contact us in case of a request, complaint, or question?

General questions about this Privacy Statement or the processing of your Personal Information can be directed to the Privacy Office at usprivacyoffice@philipsmedicalcapital.com.

To exercise your applicable privacy rights or options or file a privacy-related complaint:

Please submit your request using this form **PRIVACY OPTIONS;**

or

Contact us at **(866) 222-2478 (**Monday through Thursday from 8 a.m. to 5 p.m. CST and Friday from 8 a.m. to 4:30 p.m. CST).

PMC's Verification Process

When you make a request regarding your Personal Information, we will ask you to provide the following information to verify your identity ("Verifiable Request"):

- Name, address, phone number, date of birth, email address; and, in certain situations as may be required to confirm your identity, the last 4 digitals of your social security or individual taxpayer identification number, and/or a copy of government issued photo ID.

If you are making a request as an authorized agent for a California resident, we may request that you provide, as applicable:

- Your name, address, phone number, date of birth, email address; and, in certain situations as may be required to confirm your identity, a copy of government issued photo ID.
- The California resident's name, address, phone number, date of birth, email address, last 4 digits of social security or individual taxpayer identification number; and, in certain situations as may be required to confirm the identity of the individual on whose behalf the request is being made, a copy of a government issued photo ID.
- A document to confirm that you are authorized to make the request on the California resident's behalf. We accept as applicable: a copy of a power of attorney, legal

guardianship, conservatorship order, or the California resident's signed permission demonstrating that you are authorized to act on such California resident's behalf.

- In addition, if you are a company or organization ("Authorized Entity") making a request as an agent on behalf of a California resident:
  - Authorized Entity's active registration with the California Secretary of State.
  - From the individual who is acting on behalf of the Authorized Entity, proof that the individual is authorized to make the request. We accept a letter on the Authorized Entity's letterhead, signed by an officer of the Authorized Entity.

11 Privacy statements and other consumer privacy notices

View or download the current version of the Privacy Statement (PDF)
View or download the **PREVIOUS VERSION OF THE PRIVACY STATEMENT** Dated March 23, 2020