Privacy Statement

Effective Date: February 1, 2024

HM Electronics, Inc. and each of its affiliates (collectively, "HME", "we", "us" or "our") respect your privacy and are committed to processing your personal data in accordance with the law. This Privacy Statement (hereinafter the "Statement" or "Privacy Statement") applies to all applications, websites and domains owned by HME linking to or posting this Statement, including www.hme.com; www.hme.com/qsr; www.clearcom.com; www.clearcom50.com; www.trilogycomms.com; www.cerepairs.com; www.hmedtcloud.com; customerservice.hme.com; customerservice.cerepairs.com; and customerservice.clearcom.com ("Website" or "Websites").

This Privacy Statement describes how we collect, use, store, disclose and process personal data that we obtain through or in connection with the use of our Websites, including through or in connection with purchases of our products and services, through or in connection with use of the HME Careers Portal, the Customer Portal, the HME Cloud, our drive-thru products and services including the Zoom® and Nexeo® drive-thru systems, the Clear-Com Partner/Consultant Portal and SkyPort™, the Clear-Com Agent-IC® and Station-IC™ applications and Gen-IC™, or when you otherwise contact us and/or we collect your personal data.

HME reserves the right to change, modify and update this Privacy Statement from time to time by posting a revised version on our Websites and by revising the "Effective Date" at the top of this Statement. If considered necessary, we will also notify you directly of any change. Therefore, we recommend you regularly consult this Statement to make sure that you are aware of any changes.

1. General

1. The term "personal data" as used in this Statement shall mean any information (including "personal information" as that term may be defined in applicable privacy law) that actually enables, or is capable of enabling us to identify you, directly or indirectly, by reference to an identifier such as your name, identification number, location data, online identifier or one or more factors specific to you.
2. For the purposes of the General Data Protection Regulation 2016/679 (the "GDPR") and other laws globally, the HME entity that is responsible for your personal data ("data controller") is the HME entity from which you have purchased products and/or services, or with which you have applied for a job or entered into communications, or which has otherwise collected your personal data. For further details on each HME data controller, please see below.
3. If you have questions about this Privacy Statement or the manner in which HME collects, uses or otherwise processes your personal data, please contact the Privacy Team at the relevant HME data controller using the contact details below:

HM Electronics, Inc.
By post: 2848 Whiptail Loop, Carlsbad, CA 92010, USA
By email: Privacy@hme.com

Clear-Com LLC ("Clear-Com")
By post: 1301 Marina Village Parkway, Suite 105, Alameda, CA 94501, USA
By email: marketing@clearcom.com

Clear-Com Research Inc.
By post: 1430 Hocquart, Suite 101
St-Bruno-de-Montarville, Quebec J3V 6E1
Canada
By email: marketing@clearcom.com

with a copy to Data Protection Officer:

Marco Lopez – marco.lopez@clearcom.com

Trilogy Communications Limited
By post: 2000 Beach Drive, Cambridge Research Park, Cambridge CB25 9TP, United Kingdom
By email: trilogycomms.com/en/contact

Commercial Electronics, Inc.
By post: 3787 Rider Trail S., Earth City, MO 63045, USA
By email: Privacy@ceinstl.com

4. The Websites may, from time to time, contain links to and from the websites of our partner networks, advertisers, and other third parties. If you follow a link to any of these websites, please note that these websites may have their own privacy statements and that we do not accept any responsibility or liability for these statements. Please check these statements before you submit any personal data to these websites.

2. Careers with HME

1. HME's Careers Portal (accessible by following the 'careers' link on our applicable Websites) allows you to apply for positions with HME. Moreover, it offers you the opportunity, without application to a particular position, to submit the information that will allow HME to contact you if suitable openings arise in the future (provided you have given your consent to be contacted in such an event).

2. Registering for the Careers Portal requires you to submit specific personal data. You are under an obligation to provide only personal data which is accurate, complete and up to date at the time at which you submit it to the Careers Portal.
3. The open career opportunities published on our Websites do not constitute an offer or promise of employment and HME may eliminate, modify or change without notice any aspect(s) of the employment positions, compensation, and benefit plans described therein. Our Websites provide descriptions of possible positions within HME, and do not provide binding offers nor terms and conditions of employment. Any employment offer that may follow as a result of the identification of a potential opportunity by an applicant or submission of information to HME is in accordance with the specific terms of that offer.
4. Please note, by entering your eSignature and clicking "submit", you acknowledge and agree that your personal data will be processed in order to process your employment application in accordance with this Statement. If your application is unsuccessful, we will store your personal data for up to six (6) months (or such longer period as may be required by applicable law) in the Careers Portal following the conclusion of the unsuccessful application, in order to respond to any questions you might have about your application and in order to protect ourselves from legal claims. With your consent, we may retain your personal data for the purposes of identifying and contacting you about other suitable recruitment opportunities within HME globally for a further five (5) year period, unless you withdraw your consent or deactivate your profile, which you may do at any time. Deactivating your profile will withdraw all your applications from all the positions you have applied to within HME and will remove your profile from the Careers Portal. However, if you have applied for a position within HME, your personal data may be retained for a temporary period of time in an "inactive" status as required by applicable law and may not be deleted immediately. While you may request that we delete your personal data, we will not be able to process your job application as a result.

3. Categories of Personal Data HME Collects

1. We may collect and process the following categories of personal data:
    - **Personal data provided to us.**
      Suppliers, vendors, customers, authorized users of our products and/or services, partners and Website visitors provide personal data to us in many ways, for example by filling in online feedback and contact forms, requesting information, purchasing HME products, subscribing to materials and newsletters, participating in surveys, signing up for the Customer Portal, the HME Cloud, our drive-thru products and services including the Zoom® and Nexeo® drive-thru systems, the Clear-Com Partner/Consultant Portal and SkyPort™, the Clear-Com Agent-IC® and Station-IC™ applications and Gen-IC™. This includes personal data, such as:
        - **Identifiers**, including name, title, alias, date of birth, marital status, postal address, email address, phone number, passport number, unique personal identifiers (such as log-in details, your

username and password and customer ID) and the company you represent;
- **Commercial information**, such as transaction history, products/services purchased, obtained or considered etc.; and
- **Financial and transaction data**, including bank account and payment card details and information about payments from you and other details of products and services you have purchased from us.
- **Sensitive Personal Information,** such as Social Security or other tax identification number, financial account, debit card, or credit card number in combination with any required security or access code, or precise geolocation.

If you sign up for the Careers Portal and apply for work with us, or if you are a current or former employee, we may collect, store, and use the following categories of personal data that you have provided to us in your curriculum vitae, a covering letter, on an application form or during an interview or onboarding, or that we have received from a recruitment agency, reference, or background check provider:

- **Identifiers**, including name, title, alias, date of birth, marital status, postal address, email address, phone number, passport number, unique personal identifier, Social Security or other tax identification number, preferred job role and HME office location;
- **Protected Information** such as name with: Social security or other tax identification number, driver's license or state ID number, financial account, medical, health, and health insurance information, user name and password;
- **Protected anti-discrimination classification information,** such as age (40 years or older), race, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, pregnancy or childbirth and related medical conditions), and veteran or military status;
- **Professional or employment-related information**, such as employment history, qualifications, answers to questions about suitability for a position, preferred job conditions, extracurricular activities, professional references and professional and personal competencies;
- **Education information**, such as academic qualifications and education records;
- **Electronic network activity,** such as your use of HME systems, browsing or search history, or website interactions; and
- **Sensitive Personal Information**, such as Social Security or other tax identification number, driver's license, passport number or other government-issued identification information, account log-in, financial account, debit card, or credit card number in combination

with any required security or access code, password, or credentials allowing access to an account, precise geolocation, and consumer's racial or ethnic origin.

- **Personal data we collect.**

  We also collect the following information indirectly from you when you access our Websites, use our interactive chat function, or otherwise correspond with us by post, phone, email or otherwise:

  - **Identifiers**, such as the phone number or email address used to correspond with us;
  - **Audio, video or similar information,** such as call center phone call recordings and security camera video recordings at our facilities**;**
  - **Internet or other similar network activity**, such as limited technical information including information on your IP address, browsing or search history, website interactions, advertisement interactions, browser type and version, time zone setting and location, operating system and platform, page interaction information, and the type of device used to access our Websites; and
  - **Geolocation,** limited to town or city level information based on your IP address.

  We may collect such internet or other similar network activity data using cookies and similar technologies. When you first access our Websites from certain jurisdictions, you will receive a message advising you that cookies and similar technologies are in use. By clicking "accept cookies", you signify that you understand and agree to the use of these technologies, as described in our Cookie Notice. For more information about our practices in this area for a particular Website, please see our Cookie Notice linked in the footer of such Website.

  We may also allow select third parties to collect information about our Website visitors to provide us with better insights into the use of our Websites or user demographics or to provide relevant advertising to you. These third parties may collect information about a consumer's online activities over time and across different websites when he or she uses our Websites. Again, please see our Cookie Notice for further details.

  - Not all information is collected about all individuals. For instance, we may collect different personal data from applicants for employment or from vendors or from customers.
  - We do not knowingly collect personal data from children under the age of sixteen (16) and do not target our Websites to children

under sixteen (16). We encourage parents and guardians to take an active role in their children's online activities and interests

4. How HME uses personal data

1. We will only process your personal data in accordance with this Statement and the applicable law.
2. We will process personal data for the following purposes as is necessary for the performance of a contract between you and us or to answer questions or take steps at your request prior to entering into a contract, where you are a:
    - **Supplier, vendor, customer, authorized user of our products and/or services, partner or Website visitor, we may process your identifiers, commercial information, financial and transactional data, audio/video and electronic network activity information:**
        - To administer or otherwise carry out our obligations in relation to any agreement to which we are a party;
        - To allow you to make purchases;
        - To assist you in completing a transaction or order;
        - To allow tracking of shipments;
        - To prepare and process invoices;
        - To allow you to view and pay invoices;
        - To respond to queries or requests and to provide services and technical and sales support;
        - To provide aftersales customer relationship management;
        - To create and manage our customer accounts;
        - To notify you about changes to our services;
        - To facilitate, manage and to allow you to register a profile on the Websites, and manage your settings thereon;
        - To allow you to log into your profile to manage your settings, configure your restaurant layout, upgrade and change your plan and to change default message settings; and
        - To administer any promotion or competition.
    - **Job applicant, current and former employees only, we may process your identifiers, audio/video and electronic network activity information, geolocation, sensitive personal information, protected anti-discrimination information, professional or employment-related information and non-public education information:**
        - To facilitate, manage and to allow you to register a profile on the Careers Portal;
        - To assess your qualifications with respect to your application for a position within HME, and to decide whether to enter into an employment relationship with you; and
        - To facilitate candidate onboarding processes and manage your employment relationship with us including payroll, benefits, and expense administration, systems access and use, performance

reviews, promotions, discipline, termination and claims management.
        - We use and process protected antidiscrimination information and sensitive personal information to comply with laws including antidiscrimination laws and disability accommodation laws.
3. We will process personal data for the following purposes as necessary for certain legitimate interests, or where you have given your informed consent to such processing if required by applicable law (such consent can be withdrawn at any time), where you are a:
    - **Supplier, vendor, customer, authorized user of our products and/or services, partner or Website visitor, we may process your identifiers, commercial information, financial and transactional data and internet or other similar network activity:**
        - To offer our services to you in a personalized way, for example, we may provide suggestions based on your previous requests to enable you to identify suitable products and services more quickly;
        - To send you personalized marketing communications, in order to keep you informed of our and our selected partners' products and services, which we consider may be of interest to you;
        - To provide you, or allow selected third parties to provide you, with information about products or services, that may be of interest to you; and
        - To allow you to participate in contests and surveys and benefit from personalized promotional offers.
    - **Job applicants, current and former employees only, we may process your identifiers, protected antidiscrimination information, sensitive personal information, professional or employment-related information and non-public education information:**
        - To assess your qualifications with respect to available positions within HME, to review references and facilitate background screening and to decide whether to enter into an employment relationship with you; and
        - To contact and correspond with you regarding job applications and to contact you if your profile and preferences match a vacant position within HME, as long as your profile is active in the Careers Portal.
        - We use and process protected antidiscrimination information and sensitive personal information to comply with laws including antidiscrimination laws and disability accommodation laws
4. We will process personal data for the following purposes as is reasonably necessary for our legitimate business interests, provided such interests are not overridden by your interests or fundamental rights, where you are a:
    - **Job applicant, current or former employee, supplier, vendor, customer, authorized user of our products and/or services, partner or a Website visitor, we may process your identifiers, commercial information, financial and transactional data, professional or**

employment-related information, audio/video and internet or other similar network activity:

- To monitor, quality control and ensure compliance with any and all applicable laws, regulations, codes and ordinances, for example, in response to a request from a court or regulatory body, where such request is made in accordance with the law;
- To resolve any disputes and to protect, enforce or defend our rights;
- As part of our efforts to keep our Websites and computer systems safe and secure;
- To ensure the security of your account and our business, preventing or detecting fraud, malicious activity or abuses of our Websites and computer systems, for example, by requesting verification information in order to reset your account password (if applicable);
- To administer our Websites and computer systems for internal business administration and operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- To create products or services that may meet your needs;
- To develop and improve our products and services, for example, by reviewing user comments and visits to our Websites and various subpages to assess demand for specific products and services; and
- To measure the performance of marketing initiatives, ads, and websites "powered by" another company on HME's behalf.

- **Job applicant, current and former employees only, we may process your identifiers, professional or employment-related information, protected antidiscrimination information, sensitive personal information and non-public education information:**
  - To transfer candidate data from the Careers Portal to our internal HR systems in the event of a successful application;
  - To facilitate candidate onboarding processes and manage your employment relationship with us including payroll, benefits, and expense administration, systems access and use, performance reviews, promotions, discipline, termination and claims management; and
  - We use and process protected antidiscrimination information and sensitive personal information to comply with laws including antidiscrimination laws and disability accommodation laws.

5. We may process your personal data in order to protect your vital interests or the vital interests of another person, for example in order to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
6. Notwithstanding any legal basis for processing personal data identified above, where required by applicable law, we will obtain consent for the processing of personal data, which consent may be express or implied depending on the circumstances.

5. Clear-Com Agent-IC® and Station-IC™ Applications

1. Certain features of the Clear-Com Agent-IC® and Station-IC™ applications can and do access data from the device on which they are hosted. The Clear-Com Agent-lC® and Station-IC™ applications send audio data to (i) the Clear-Com intercom system, (ii) the Clear-Com Gen-IC™, if purchased by the customer, and (iii) third party equipment and software managed by the user, to the extent such equipment and software is connected to the applicable audio ports, including operating software and other software on the user's device, and third party devices and systems managed by the user. Audio data that is transmitted by the Clear-Com Agent-IC® and Station-IC™ applications to the Clear-Com intercom system implemented by the user will be encrypted using AES-128 technology and only established upon successful key exchange using the user's encrypted password for added security.
2. The Clear-Com Agent-lC® and Station-IC™ applications automatically check for the latest versions of each application from time to time using a Clear-Com managed service operated on behalf of Clear-Com. If a new version is identified, the user will be prompted to download and install the new version of the relevant application.
3. The Clear-Com Agent-lC® and Station-IC™ applications store user profiles including network addresses, usernames and passwords needed for the applications to access the intercom system locally on the device that runs the applications. The Clear-Com Agent-IC® and Station-IC™ applications allow users to store such profiles and data on Gen-IC™ or other cloud service operated on behalf of Clear-Com. Access to the optional cloud storage feature is controlled on behalf of Clear-Com using a third party authentication mechanism, and may be tied to the customer's single sign-on (SSO) authentication service.
4. The Clear-Com Agent-IC® and Station-IC™ applications may collect data for the purpose of providing technical support including usage data, operating system and platform, device type, device or host name, username, application version and configuration data ("Support Data"). Users can choose to store Support Data on the user's computer or other device. Users can also upload a copy of the Support Data with a support request, which Clear-Com may access to provide support services requested.
5. The Clear-Com Agent-IC® and Station-IC™ applications may collect technical data on the performance of the applications including usage data, operating system and platform, application version, device type, and location ("Technical Data"). This Technical Data may be aggregated by or on behalf of Clear-Com and is used to measure user engagement and may be used to develop and improve the application but is not associated with other identifiers.
6. While certain other features of the applications may have access to other personal or sensitive user data from your device, neither Clear-Com nor the applications collect, transmit, store or otherwise use such data.
7. Access to the Clear-Com Agent-lC® and Station-IC™ applications may be managed by or on behalf of Clean-Com using third party licensing software.

6. Drive-thru products and services

1. We may from time to time offer products and services to our customers which enable them to, amongst other things:
    - enable their staff members to record and send voice notes;
    - monitor the performance of drive-thru services;
    - use sensors to trigger alerts when actions are required;
    - provide curbside services;
    - deliver voice-activated services, including to enable automated order taking systems; and
    - monitor interactions between staff members and consumers for quality and training purposes.
2. These products and services may collect personal data relating to individuals which we may combine with technical performance data to provide analytics and other services to our customers. Our customers are responsible for ensuring that their use of these products and services, and their collection and processing of personal data, complies with all applicable privacy laws.
3. The above data is hosted in HME Cloud servers located in the United States. By accessing HME Cloud from outside the United States, you acknowledge that your personal data will be accessed by us and stored in the United States.

7. The Zoom® and Nexeo® drive-thru system in HME Cloud

1. To provide the Zoom® and Nexeo® drive-thru system in HME Cloud, we collect two main categories of data:
    - drive-thru performance data (e.g., data relating to the time it takes to fulfil drive-thru orders). We use this data to provide dashboards and analytics within HME Cloud. Performance data does not contain personal data and does not relate to individual employees or any other identified persons; and
    - identifiers, including name and email address provided by, or on behalf of, authorized users when they sign up to access the performance data, dashboards and analytics within HME Cloud. This data contains personal data and relates to the individual authorized users. We process this data to provide the Zoom® and Nexeo® drive-thru system in HME Cloud in accordance with this Statement and applicable law.
2. The above data is hosted in HME Cloud servers located in the United States. By accessing HME Cloud from outside the United States, you acknowledge that your personal data will be accessed by us and stored in the United States.

8. How long HME retains personal data

1. We will store your personal data, in a form that permits us to identify you, for no longer than is necessary for the purpose for which the personal data is processed. We store your personal data as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements and rights, or if it is not technically and reasonably feasible to remove it. Otherwise, we will seek to delete your personal data within a reasonable timeframe upon request.
2. If you choose a direct payment gateway to complete a purchase on the Websites, then PayPal Gateway stores your credit card data. Your purchase transaction data

is stored in accordance with PayPal's retention practices.

9. Where HME stores personal data

1. We are headquartered in the United States. Your personal data will be stored on secure servers and will be accessed by us (including our authorized personnel) or transferred to us in the United States or to our affiliates, partners, or service providers who are located worldwide. By visiting our Websites from outside the United States, you acknowledge that your information may be transferred to, stored, and processed in the United States where our servers are located, and our central database is operated, as well as other countries where our service providers, partners or affiliates are located.
2. Where personal data is transferred from the European Economic Area or Switzerland to a country that has not received an adequacy decision by the European Commission, we rely on appropriate safeguards, such as the European Commission-approved Standard Contractual Clauses, as well as any supplementary measures that may be necessary, to transfer the data in compliance with applicable law.

10. How HME shares personal data

1. We will not sell, hire out, disclose, transfer or pass on your personal data to third parties, except in the situations provided for in this Statement or unless you provide prior consent. We may share personal data in the following ways:
    - **Our Affiliates.** Your personal data may be accessed by us or transferred to us in the US and shared with our affiliates in order to process your personal data (the information shared includes identifiers, commercial information, financial and transaction data, internet or other similar network activity, professional or employment-related information and non-public education information). Such information may be shared so that affiliates can provide and share services relating to (amongst other things) HR, finance, customer care, quality review and management of vendors, distributors, partners, suppliers, contractors and others, compliance with regulatory bodies and public authorities, supply chain and sourcing management, tendering, quoting and bidding for any private, public or governmental projects, and implementing and sharing information on the same, sales administration, technology services including research and development, business development, marketing activities and preparing business plans, IT, risk management, database management and analysis of commercial activities, administrative services, accounts and records, tax planning and compliance services, and marketing services.
    - **Third-party service providers.** We may share personal data with service providers and suppliers retained to deliver complete products, services and customer solutions and to assist us with marketing and communication initiatives, and service providers retained to assist us with staffing and employee administration. These service providers and suppliers include, for example, providers of site and store hosting services, providers of

voice activated input/output software and related technology for automated order taking systems, customer support and live-help, IT and network vendors, marketing, email service providers, automated data processors, providers of payment processing and payroll services, employee benefits providers, and shipping agents. When we share your personal data with third parties that we engage to process data on our behalf, including our affiliates, we will ensure that those third parties are contractually bound to guarantee the same levels of privacy protection and confidentiality observed by HME when handling your personal data (the information shared includes identifiers, commercial information, financial and transaction data, protected information, internet or other similar network activity, professional or employment-related information and non-public education information).

- **Resellers and agents.** We may share personal data with, and receive personal data from, our dealers, distributers, agents and resellers in order to fulfil orders and facilitate repairs of faulty HME products (the information shared includes identifiers, commercial information and financial and transaction data).
- **Third party involved in a business transaction.** We may share personal data with one or more third parties in connection with or during negotiation of any merger, financing, acquisition or dissolution, transition, or proceeding involving the sale, transfer, divestiture, or disclosure of all or a portion of our business or assets. In the event of an insolvency, bankruptcy or receivership, such personal data may also be transferred as a business asset. If another company acquires any of our companies, businesses or assets, that acquiring company may acquire your personal data, and in that case, we will inform you of the new controller responsible for the protection of your personal data. We do not guarantee that any entity receiving such data in connection with one of these transactions will comply with all of the terms of this Statement following such transaction. However, it is our practice to seek reasonable protection for personal data in these types of transactions (the information shared may include identifiers, commercial information, financial and transaction data, internet or other similar network activity, professional or employment-related information and non-public education information).
- **Our advisors.** We may share your personal data with our auditors, legal advisors, and similar third parties in connection with our receiving their professional services, subject to standard confidentiality obligations (the information shared may include identifiers, commercial information, financial and transaction data, internet or other similar network activity, professional or employment-related information, non-public education information and sensitive personal information).
- **Law enforcement.** We may disclose personal data to the government or to third parties under certain circumstances when legally obligated to do so, such as in connection with suspected illegal activity concerning our Websites, products or services, or to respond to a subpoena, court order or other legal processes, or that we believe may aid a law enforcement investigation. In accordance with applicable law, we reserve the right to

release personal data to law enforcement or other government officials, as we, in our sole discretion, deem necessary or appropriate (the information shared may include any category of information we collect).

- **Legal processes.** We may share all types of personal data with others as required by, or permitted by, applicable law. This may include sharing personal data with governmental entities, or third parties in response to subpoenas, court orders, other legal processes, or as we believe is necessary to exercise our legal rights, to defend against legal claims that have been brought against us, to defend against possible legal claims that we determine in our sole discretion might be brought against us, to investigate and help prevent security threats, fraud or other malicious activity and to protect the rights or personal safety of HME employees and third parties (the information shared may include all categories of information we collect).
- **Other Third Parties.** We may share aggregated and/or anonymized data with other third parties that are not described above. When we do so, we will either aggregate or anonymize the data so that a third party cannot link data to you, your computer, or your device. Aggregation means that we combine the information of numerous people together so that the data does not relate to any one person. Anonymization means that we remove or change certain pieces of information in such a way that the you are no longer identifiable.

11. Your rights as a data subject

1. General rights
    - If any of the personal data that we have about you is incorrect, or you wish to have personal data removed from our records, please contact us using the contact details provided above, or log into your account where relevant.
    - Additionally, if you prefer not to receive marketing messages or information about vacant job positions from us, please let us know by clicking on the unsubscribe link within any such message that you receive, or by sending a message to us using the contact details above. You are able to opt-out of receiving marketing messages from us. However, you cannot opt-out of receiving all emails from us, such as emails about the status of your account or the status of an order for a product you have placed with us.
2. European data subject rights

    If you are a resident of the European Union, you may have the following rights in relation to your personal data:

    - **Request access to your personal data.**
    - **Request correction of your personal data.**
    - **Request erasure of your personal data.**
    - **Request restriction of processing your personal data.**

- **Request transfer of your personal data.**
- **Right to object.**
- **Right to withdraw consent.**
- **Right to complain.**

Exercising your rights

To exercise the above-mentioned rights, or to raise a question, comment or complaint, send an email with an enclosed copy of the front side of your identity card, driving license or passport to the Privacy Team at the relevant HME data controller using the contact details above. We reserve the right to request the provision of additional information necessary to confirm the identity of the enquirer.

3. Privacy rights for residents of California only

Shine the Light Under California law, a California customer with whom HME has an established relationship has the right to request certain information with respect to the types of personal data that we have shared with third parties for direct marketing purposes and the identities of those third parties during the prior calendar year.

Exercising your rights

To exercise your Shine the Light rights, or to raise a question, comment or complaint, send an email with an enclosed copy of the front side of your identity card, driving license or passport to the Privacy Team at the relevant HME data controller using the contact details above. We reserve the right to request the provision of additional information necessary to confirm the identity of the enquirer.

4. California Privacy Rights Act Rights for residents of California only

The California Privacy Rights Act ("CPRA") provides "consumers" (California residents) with specific rights regarding their "personal information." This section describes your CPRA rights and explains how to exercise those rights.

During the previous twelve (12) months, we have collected the categories of personal information listed in Section 3 of this Statement, used the categories of personal information listed in Section 4 of this Statement, and disclosed the categories of personal information listed in Section 10 of this Statement for a business purpose.

Processing Sensitive Personal Information

We collect and process Sensitive Personal Information for the purposes disclosed at the time we collect this information. We do not process this information for purposes other than the purpose for which it was originally collected unless required by law. We use and process Sensitive Personal Information collected from California employees, job applicants or vendors (including racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status) to comply with laws including anti-discrimination laws and disability accommodation laws. We use Sensitive Personal Information from other consumers (including racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status) to provide disability accommodations.

Sale of personal information

We do not sell personal information for monetary consideration but we may transfer your information to a third party that provides us with services such as helping us with advertising, data analysis and analytics, and security, which may fall under the definition of for "other valuable consideration" and which may therefore be considered a "sale" under the CPRA. In the preceding twelve (12) months, HME has sold the following categories of personal information:

- Identifiers;
- Commercial information;
- Internet or other similar network activity;
- Professional or employment-related information;
- Non-public education information; and
- Inferences drawn from other personal information.

Sharing personal information for cross-context or behavioral marketing purposes.

We do not share personal information with third parties who may use it for cross-context or behavioral advertising purposes.

Your rights and choices

Verified California residents have the right to obtain certain information about our collection and use of personal information over the past twelve (12) months, including:

- The categories of personal information we collect;
- The categories of sources of personal information we collect;
- Our business purpose for collecting or sharing that personal information;
- The categories of third parties with whom we share that personal information;

- The specific personal information we have collected about you over the past twelve (12) months, or, at your option since January 1, 2022 ("Data Portability");
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
    - the categories of personal information sold and the category of third party recipients; and
    - list of the categories of personal information that we disclosed for a business purpose.

You have the right to request that we correct information about you that is not correct, to request that we do not sell personal information about you, to request that we do not process sensitive personal information about you for any purposes other than those for which the information was originally collected, and to request that we delete (and direct our service providers to delete) your personal information subject to certain exceptions.

Exercising Personal Information Sales Opt-Out and Opt-In Rights; Limit Processing of Sensitive Information Opt-out

If you are sixteen (16) years of age or older, you have the right to direct us to not sell your personal information at any time (the "right to opt-out"). We do not sell or share the personal information of individuals we actually know are less than sixteen (16) years of age. To exercise the right to opt-out, you (or your authorized representative) may submit a request to us by visiting the following page: Do Not Sell My Personal Information and Limit Processing of Sensitive Information. You may exercise this right at any time.

You may also opt out by activating a user-enabled global privacy control, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicates or signals your choice to opt-out of the sale of personal information. When we receive such a signal we will stop setting third party, analytics, or advertising partner cookies on your browser. This will prevent the sale of information relating to that specific device through cookies to our advertising or analytics partners. This option does not stop all sales of your information because we cannot match your device's identification or internet protocol address with your personally identifiable information like your name, phone number, email address or ZIP Code. If you delete cookies on your browser, any prior do not sell or do not share signal is also deleted and you should make sure that your user-enabled setting is always activated.

Once you make an opt-out request, we will wait at least twelve (12) months before asking you to reauthorize personal information sales.

We do not share personal information for behavioral or cross-context marketing purposes and do not process sensitive personal information for purposes other than those for which it was originally collected.

Exercising your rights for Information Collection or Disclosure Practices, Data Portability, Correction or Deletion

You can exercise any of these rights by contacting us using the contact details set out above or you may submit a request to us by visiting the following page Website Request Page. You may also call us on the following toll free telephone number: **800-978-3514**. You may make a request for Information Collection or Disclosure Practices or Data Portability up to twice within a twelve (12) month period; the disclosure we provide will cover the twelve (12) months prior to your request or, at your option, since January 1, 2022. You may make deletion or correction requests at any time.

We will ask you for information that allows us to reasonably verify your identity (that you are the person about whom we collected personal information) and we will use that information only for that purpose. We may request that you submit a signed statement under penalty of perjury that you are the individual you claim to be. We cannot respond to your request or provide you with personal information if we cannot verify your identity and confirm that the personal information relates to you.

Response timing and format

We will acknowledge receipt of your request for information collection or disclosure practices, data portability, correction or deletion within ten (10) business days and will endeavor to respond within forty-five (45) days of receipt of your request, but if we require more time (up to an additional forty-five (45) days) we will notify you of the reason and extension period in writing.

For requests that we not sell or share your information or limit processing of Sensitive Personal Information we will comply with your request promptly, and at least within fifteen (15) business days.

Where you request a copy of your personal information, we will endeavor to provide the information in a format that is readily useable, including by mailing you a paper copy or providing an electronic copy.

We do not charge a fee to process or respond to your request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request. We will not discriminate against you as a result of your exercise of any of these rights.

5. Notice to Nevada Residents.

   If you would like to tell us not to sell your information please email us at privacy@hme.com with your name, postal address, telephone number and email address with "Nevada do not sell" in the subject line.

6. Privacy Rights for Canadian Residents

   If you are a resident of Canada, you may have the following rights in relation to your personal data:

   - **Request access to your personal data and receive information about how it has been processed.**
   - **Request correction of your personal data.**
   - **Request erasure of your personal data in limited circumstances.**
   - **Right to withdraw consent.**
   - **Right to complain.**

   Exercising your rights

   To exercise the above-mentioned rights, or to raise a question, comment or complaint, send an email to the Privacy Team at the relevant HME data controller using the contact details above. We reserve the right to request the provision of additional information necessary to confirm the identity of the enquirer.

12. Safety and Confidentiality

1. HME takes steps to maintain the security of your personal data and to prevent unauthorized access to it through the use of appropriate technology and internal procedures.
2. If you choose a direct payment gateway to complete your purchase, then PayPal Gateway stores your credit card data. PayPal Gateway is encrypted through the Payment Card Industry Data Security Standard ("PCI-DSS"). All direct payment gateways adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of credit card information by our store and its service providers.