Privacy Policy

Last updated: July 11, 2018

Protecting your privacy is very important to us. We're telling you about our privacy policy and notice so you know what information we collect, why we collect it, and what we do with it. The Embleema Service ("Service") is owned and operated by Embleema Inc. ("Embleema", "us", "we", or "our"), a Delaware corporation. We operate the www.embleema.com as well as the patienttruth.embleema.com website (collectively the "Website"). Your use of the Website and Service is governed by the privacy policy and notifications contained herein together (the " Privacy Policy", "Policy"). Please read this Privacy Policy carefully. By accessing, browsing or otherwise using the Website or any Embleema Service, you acknowledge that you have read, understood, and agree that you have been so notified of this Privacy Policy. If you do not accept the terms and conditions of this Privacy Policy, you should not access, browse or use the Website. This page informs you of our policies regarding the collection, use and disclosure of Personal Information when you use our Service.

We will not use or share your information with anyone except as described in this Privacy Policy.

We use your Personal Information for providing and improving the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions, accessible at our Website.

1. Information Collection and Use

1.1. While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to, your first name, last name, address and email address ("Personal Information"). We collect this information for the purpose of providing the Service, identifying and communicating with you, responding to your requests/inquiries, servicing your purchase orders, and improving our services. We do not collect social security number or other similar information unless you choose to provide it. We do collect other limited information automatically from visitors who read, browse, and download information from our site. We do this, so we can understand how the site is being used and how we can make it more helpful.

1.2. Certain information about your visit can be collected when you browse websites. When you browse the Embleema Website, we, and in some cases our third-party service providers, can collect the following types of information about your visit, including:

- Domain from which you accessed the Internet

- IP address (an IP or internet protocol address is a number that is automatically assigned to a device connected to the web)
- Approximate geographic location based on the IP address of the user's local system
- Operating system (which is software that directs a computer's basic functions such as executing programs and managing storage) for the device that you are using and information about the browser you used when visiting the site
- Date and time of your visit
- Pages you visited
- Address of the website that connected you to our Website (such as google.com or bing.com)
- Device type (desktop computer, tablet, or type of mobile device)
- Screen resolution
- Browser language
- Geographic location
- Time spent on page
- Scroll depth – The measure of how much of a web page was viewed
- User events (e.g. clicking a button)
- We use this information to measure the number of visitors to our site and its various sections, to help make our site more useful to visitors.

2. Cookies

2.1. When you visit a website, its server may generate a piece of text known as a "cookie" to place on your device. The cookie, which is unique to your browser, allows the server to "remember" specific information about your visit while you are connected. There are two types of cookies, single session (temporary), and multi-session (persistent). Single session cookies last only as long as your web browser is open. Once you close your browser, the session cookie disappears. Persistent cookies are stored on your device for longer periods. Both types of cookies create an ID that is unique to your device.

2.2. Session Cookies: We use session cookies for technical purposes such as to allow better navigation through our site. These cookies let our server know that you are continuing a visit to our site.

2.3. Persistent Cookies: We use persistent cookies to understand the differences between new and returning visitors to the Embleema website. Persistent cookies remain on your device

between visits to our site until they expire or are removed by the user. We do not use persistent cookies to collect personally identifiable information. Embleema does not identify a user by using such technologies.

2.4. The cookie makes it easier for you to use the dynamic features of Embleema. Information that you enter into the application is not associated with cookies on Embleema. Depending on the third-party tool's business practices, privacy policies, terms of service, and/or the privacy settings you selected, information you have provided to third parties could be used to identify you when you visit the Embleema website. These third parties do not/will not share your identity with Embleema.

2.5. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. The Help feature on most browsers provide information on how to accept cookies, disable cookies or to notify you when receiving a new cookie. If you do not accept cookies, you may not be able to use some features of our Service and we recommend that you leave them turned on.

3. Do Not Track Disclosure

3.1. Do Not Track ("DNT") is a preference you can set in your web browser to inform websites that you do not want to be tracked.

3.2. Embleema automatically observes the DNT browser setting for digital advertising that uses "conversion-tracking" or "re-targeting". If "Do Not Track" is set before a device visits the Embleema website, third party conversion tracking and retargeting tools will not load on the site. For more information on DNT or information on how to set the Do Not Track setting in your browser go to the Do Not Track website.

3.3. So you can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser.

4. Service Providers

4.1. We may employ third party companies and individuals to facilitate our Service, to provide the Service on our behalf, to perform Service-related services and/or to assist us in analyzing how our Service is used. We will only share PII with third party vendors, consultants, agents, partners, and other service providers with whom we contract to help us provide or improve our services.

4.2. These third parties have access to your Personally Identifiable Information ("PII") only to perform specific tasks on our behalf and are obligated not to disclose or use your information for any other purpose.

4.3. Please note that Embleema will only share your information in accordance with this Policy, except in the following situations:

- You have given us your consent to share or use information about you;
- We believe that we need to share information about you to provide a service that you have requested from us or from others;
- We are required by law to disclose information; or
- We believe that it is necessary to protect our rights or to avoid liability or violations of the law.

5. Communications

5.1. We may use your Personal Information to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you.

5.2. We also engage certain service providers for purposes of tracking and associating internet search and browsing behavior to provide improved functionality on the Embleema website. We enable them to use tracking technologies, such as cookies and web beacons, on or in conjunction with the Embleema website. These companies may use non-personally identifiable information about your visits to other websites, together with non-personally identifiable information about your purchases and interests from other online and offline sources, to provide you with newsletters, marketing or promotional materials and goods and services that may be of interest to you.

5.3. The use and collection of information by these service providers is governed by their respective privacy statements and thus is not covered by this Policy. In addition, we may share Website usage information with these service providers to manage and target ads and for market research purposes.

5.4. Finally, information obtained through these processes may be combined with personally identifiable information in order to analyze our marketing efforts. You may opt out of receiving any, or all, of these communications from us by contacting us.

6. Compliance with Laws

6.1. Embleema recognizes it may be subject to the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the regulations set forth thereunder at 45 C.F.R. Part 160 and Part 164 (the "HIPAA Privacy Regulations") because Embleema provides certain services which involve (i) the use and disclosure of Protected Health Information (as defined in the HIPAA Privacy Regulations) by Embleema, and (ii) the disclosure of Protected Health Information by or on behalf of registered user by Embleema. Accordingly, pursuant to the HIPAA Privacy Regulations, Service Company may be a "Business Associate" (as defined in the HIPAA Privacy Regulations). Embleema complies with all of the requirements of HIPAA and the HIPAA Privacy Regulations applicable to Business Associates respectively.

6.2. Additionally Embleema complies in all material respects with all federal and state-mandated regulations, rules, or orders applicable to the services provided herein, including but not limited to regulations promulgated under Title II, Subtitle F of the Health Insurance Portability and Accountability Act (Public Law 104-91) ("HIPAA"). We will not disclose your Personal Information unless required to do so by law or subpoena or if we believe that such action is necessary to comply with the law and the reasonable requests of law enforcement or to protect the security or integrity of our Service. These regulations may require us to disclose to proper authorities information related to your usage of the Service, such as - but not limited to - time and date of your registration, your logins and logouts, your changes of passwords to the Service, time and date of your CCD and Fitbit uploads and authorizations to release your medical history.

7. Security

7.1. Embleema acknowledges that, during its engagement by registered users, it will have access to Personal Information including identity attributes and health information. Embleema in its collection, receipt, transmission, storage, disposal, use and disclosure of such Personal Information will be a responsible keeper of that information.

7.2. While no method of internet transmission, or electronic storage is totally secure, Embleema strives to implement and maintain reasonable, commercially acceptable security procedures and practices appropriate to the nature of the information we store. Embleema shall implement administrative, physical and technical safeguards to protect Personal Information that are no less rigorous than accepted industry practices (including the International Organization for Standardization's standards: ISO/IEC 27001:2005 – Information Security Management Systems – Requirements and ISO-IEC 27002:2005 – Code of Practice for International Security Management, other applicable industry standards for information security), and shall ensure that all such safeguards, including the manner in which Personal Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Privacy Policy.

8. International Transfer

Your information, including Personal Information, may be transferred and maintained on computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction. If you are located outside United States and choose to provide information to us, please note that we transfer the information, including Personal Information, to United States and process it there. Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

9. Changes to this Privacy Policy

Embleema may amend this Privacy Policy from time to time, at its sole discretion. Use of information we collect now is subject to the Privacy Policy in effect at the time such information is used. If we make changes to the Privacy Policy, we will notify you by posting an announcement on the Embleema website so you are always aware of what information we collect, how we use it, and under what circumstances if any, it is disclosed.

10. Embleema users located in the European Data Region

For Embleema users located in the European Data Region, all processing of Personal Data is performed in accordance with privacy rights and regulations following the EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (the Directive), and the implementations of the Directive in local legislation. From May 25th, 2018, the Directive and local legislation based on the Directive will be replaced by the Regulations (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, known as the General Data Protection Regulation (GDPR), and Embleema 's processing will take place in accordance with the GDPR.

11. Embleema users located in the US Data Region

For Embleema users in the Embleema US Data Region, Embleema processes data solely in data centers located in the US. Embleema has adopted reasonable physical, technical and organizational safeguards which substantially mirror the EU safeguards against accidental, unauthorized or unlawful destruction, loss, alteration, disclosure, access, use or processing of the user's data in Embleema 's possession. Embleema will promptly notify the user in the event of any known unauthorized access to, or use of, the user's data.

12. Users located in European Data Region: Embleema as Controller

12.1. Embleema processes Personal Data both as a Processor and as a Controller, as defined in the Directive and the GDPR:

12.2. Embleema adheres to the Directive of 1995 and the GDPR from May 25th, 2018.

12.3. All data collected by Embleema will be stored exclusively in secure hosting facilities provided by GDPR compliant Microsoft Azure. Embleema has a data processing agreement in place with its provider, ensuring compliance with the Directive. All hosting is performed in accordance with the highest security regulations. All transfers of data internally in the EEA is done in accordance with this data processing agreement.

12.4. See the EMBLEEMA GDPR DATA PROCESSING ADDENDUM

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the effected parties unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the affected parties is not made within 72 hours, it shall be accompanied by reasons for the delay.

13. Retention and Deletion

Embleema will not retain data longer than is necessary to fulfill the purposes for which it was collected or as required by applicable laws or regulations. For user data, users have control of the purpose for collecting data, and the duration for which the Personal Data may be kept.

14. Conditions of Use

We assume that all users of our Website and platform have carefully read this document and agree to its contents. If someone does not agree with this privacy policy, they should refrain from using our Website and platform. We reserve the right to change our privacy policy as necessity dictates. Continued use of Embleema's Website and platform after having been informed of any such changes to these conditions implies acceptance of the revised privacy policy. This privacy policy is an integral part of Embleema 's terms of use.

15. Links to Other Sites

Your activity on the third-party websites that Embleema links to (such as Facebook or Twitter) is governed by the security and privacy policies of those websites. You should review the privacy policies of all websites before using them so that you understand how your information may be used. We have no control over, and assume no responsibility for the content, privacy policies or practices of any third party sites or services. You should also adjust privacy settings on your account on any third-party website to match your preferences.

16. Children's Privacy

Embleema is committed to protecting the privacy of children who visit our Embleema website. Only persons age 18 or older have permission to access our Service. We do not knowingly collect personally identifiable information from persons under 18. Embleema follows the U.S. Children's Online Privacy Protection Act ("COPPA"). For more information about COPPA, please visit https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online.

17. Changes to This Privacy Policy

We may revise this Privacy Policy from time to time. The most current version of the policy dated July 11, 2018 will govern our use of your information and will always be at embleema.com/privacy. If we make a change to this policy that, in our sole discretion, is material, we will notify you via email to the email address associated with your account and/or prominent notice on our Embleema website. By continuing to access or use the Services after those changes become effective, you agree to be bound by the revised Privacy Policy.

18. Contact Us

Thoughts or questions about this Privacy Policy? Please let us know by contacting us at support@embleema.com

GDPR Data Processing Addendum

Last updated: July 11, 2018

This Data Processing Addendum ("DPA") is an agreement between Embleema ("EMBLEEMA," "we," "us," or "our") and you ("Customer", "user" or "you").

1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by EMBLEEMA. In this context, EMBLEEMA will act as "processor" and "controller" to Customer who may act as "controller" with respect to Customer Data (as each term is defined in the GDPR).

1.2 **Customer Controls.** The Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Data.

1.3 Details of Data Processing.

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.

1.3.2 **Duration.** As between EMBLEEMA and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 **Nature of the processing:** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5 **Type of Customer Data:** Customer Data uploaded to the Services under Customer's EMBLEEMA accounts.

1.4 **Categories of data subjects.** The data subjects may include Customer's customers, employers, suppliers and end-users.

1.5 **Compliance with LAW**. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. Customer Instructions. The parties agree that this DPA constitute Customer's documented instructions regarding EMBLEEMA's processing of Customer Data ("**Documented Instructions**"). EMBLEEMA will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between EMBLEEMA and Customer, including agreement on any additional fees payable by Customer to EMBLEEMA for

carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if EMBLEEMA declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

3. Confidentiality of Customer Data. EMBLEEMA will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends EMBLEEMA a demand for Customer Data, EMBLEEMA will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, EMBLEEMA may provide Customer's basic contact information to the government body. If compelled to disclose Customer Data to a government body, then EMBLEEMA will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless EMBLEEMA is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Section 3 varies or modifies the Standard Contractual Clauses.

4. Confidentiality Obligations of EMBLEEMA Personnel. EMBLEEMA restricts its personnel from processing Customer Data without authorization by EMBLEEMA as described in the EMBLEEMA Security Standards. EMBLEEMA imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Security of Data Processing

5.1 EMBLEEMA has implemented and will maintain the technical and organizational measures for the EMBLEEMA Network as described in the EMBLEEMA Security Standards and this Section. In particular, EMBLEEMA has implemented and will maintain the following technical and organizational measures:

(i) security of the EMBLEEMA Network;

(ii) physical security of the facilities;

(iii) measures to control access rights for EMBLEEMA employees and contractors in relation to the EMBLEEMA Network; and

(iv) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by EMBLEEMA.

6. Security Breach Notification.

6.1 **Security Incident.** EMBLEEMA will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and b) take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

6.2 **Unsuccessful Security Incidents.** Customer agrees that:

(i) An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of EMBLEEMA's equipment or facilities

storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and EMBLEEMA's obligation to report or respond to a Security Incident is not and will not be construed as an acknowledgement by EMBLEEMA of any fault or liability of EMBLEEMA with respect to the Security Incident.

6.3 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's contacts by any means EMBLEEMA selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information on the EMBLEEMA management console and secure transmission at all times.

7. EMBLEEMA Certifications and Audits.

EMBLEEMA ISO-Certification and SOC Reports. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, EMBLEEMA will make available the following documents and information: the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by EMBLEEMA that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

7.1 **EMBLEEMA Audits.** EMBLEEMA uses external auditors like securitymetrics.com to verify the adequacy of its security measures, including the security of the physical data centers from which EMBLEEMA provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at EMBLEEMA's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be EMBLEEMA's Confidential Information.

7.2 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, EMBLEEMA will provide Customer with a copy of the Report so that Customer can reasonably verify EMBLEEMA's compliance with its obligations under this DPA.

8. Transfers of Personal Data.

8.1 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if

EMBLEEMA has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

9. **Termination of the DPA.** This DPA shall continue in force until the termination of the Agreement (the "**Termination Date**").

10. **Return or Deletion of Customer Data**. The Services provide Customer with controls that Customer may use to retrieve or delete Customer Data as described in the Documentation. Up to the Termination Date, Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this Section. For 90 days following the Termination Date, Customer may retrieve or delete any remaining Customer Data from the Services, subject to the terms and conditions set out in the Agreement, unless prohibited by law or the order of a governmental or regulatory body or it could subject EMBLEEMA or its Affiliates to liability. No later than the end of this 90 day period, Customer will close all EMBLEEMA accounts. EMBLEEMA will delete Customer Data when requested by Customer by using the Service controls provided for this purpose by EMBLEEMA.

11. **Entire Agreement; Conflict**. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will control.

12. **Definitions.** Unless otherwise defined in the Agreement, all Capitalized terms used in this DPA will have the meanings given to them below:

"**EMBLEEMA Network**" means EMBLEEMA's data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within EMBLEEMA's control and are used to provide the Services.

"**EMBLEEMA Security Standards**" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Annex 1.

"**Customer**" means you or the entity you represent.

"**Customer Data**" means the "personal data" (as defined in the GDPR) that is uploaded to the Services under Customer's EMBLEEMA accounts.

"**EEA**" means the European Economic Area.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"**Security Incident**" means a breach of EMBLEEMA's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Standard Contractual Clauses" means Annex 2, attached to and forming part of this

DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

EMBLEEMA Security
Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. **Information Security Program.** EMBLEEMA will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the EMBLEEMA Network, and (c) minimise security risks, including through risk assessment and regular testing. EMBLEEMA will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1 **Network Security.** The EMBLEEMA Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. EMBLEEMA will maintain access controls and policies to manage what access is allowed to the EMBLEEMA Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. EMBLEEMA will maintain corrective action and incident response plans to respond to potential security threats.

   1.2 **Physical Security**

      1.2.1 **Physical Access Controls.** Physical components of the EMBLEEMA Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

      1.2.2 **Limited Employee and Contractor Access.** EMBLEEMA provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are

promptly revoked, even if the employee or contractor continues to be an employee of EMBLEEMA or its Affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. EMBLEEMA also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. EMBLEEMA will conduct periodic reviews of the security of its EMBLEEMA Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. EMBLEEMA will continually evaluate the security of its EMBLEEMA Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.