		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 1 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

1 Purpose

This policy sets forth confidentiality, security and privacy requirements with respect to Personal Information and Protected Health Information processed by MolecularMD to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Safe Harbor framework.

Molecular MD complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland.

MolecularMD has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view MolecularMD's certification, please visit <http://www.export.gov/safeharbor/>

2 Scope


This privacy policy applies to all Personal Information (PI), Sensitive Information and Protected Health Information (PHI) as defined below that is received by MolecularMD from the European Economic Area (which includes the twenty-seven member states of the European Union (EU) plus Iceland, Liechtenstein, Norway and from Switzerland) in any format, including but not limited to, electronic, paper or verbal.

3 Related Documents

3.1	Business Continuity Plan	SOP-0078
3.2	Complaint Management	SOP-0115
3.3	Computer and Network Access Set-Up	FRM-0456
3.4	Employee Confidentiality Information Agreement	FRM-0010
3.5	Facility Access and Security	POL-0003
3.6	HIPAA Confidentiality Agreement	FRM-0363
3.7	MolecularMD Business Continuity Planning	POL-0013
3.8	Organizational Chart	AI-0005
3.9	Periodic Review	SOP-0002
3.10	Quality Assurance Auditing	SOP-0009
3.11	Software, System, & Network Access Security	SOP-0133

4 Definitions, Acronyms, Abbreviations

- 4.1 Agreement:** The entire contract between the client and MolecularMD under which MolecularMD performs services for the client. An Agreement may be formed through the execution of a written contract by both parties, by MolecularMD's express or implied acceptance of a purchase order, work order, scope of work, or by any other means of offer and acceptance of a contract.


		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 2 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

- 4.2 EEA:** European Economic Area. The EEA includes the twenty-seven member states of the European Union (EU) plus Iceland, Liechtenstein, Norway and from Switzerland.
- 4.3 EU Data Protection Authorities (EU DPAs):** Authorities tasked with the protection of data and privacy in the European Union.
- 4.4 EU:** European Union
- 4.5 IRM:** Independent Recourse Mechanism
- 4.6 Personal Information (PI):** Any information provided by clients or collected by MolecularMD: (1) that identifies an individual, or when used in combination with other information identifies an individual; or (2) from which identification or contact information of an individual person can be derived. PI can be in any media or format, including computerized or electronic records as well as paper-based files. PI does not include the name, business telephone number, business cell phone number, business address, business email address, or internal identification number of individual MolecularMD employees.
- Personal Information includes, but is not limited to: (1) a first or last name or initials; (2) a home or other physical address, including street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (4) a telephone number; (5) a social security number, tax ID number or other government-issued identifier; (6) an Internet Protocol ("IP") address or host name that identifies an individual; (7) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; (8) birth dates or treatment dates; or (10) coded data that is derived from PI. Additionally, to the extent any other information (such as, but not limited to, case report form information, clinical trial identification codes, personal profile information, IP addresses, other unique identifier, or biometric information) is associated or combined with PI, then such information also will be considered PI.
- 4.7 Processing:** Any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking or dispersed erasure, or destruction.
- 4.8 Protected Health Information (PHI):** A subset of Personal Information that includes individually identifiable health information. Individually identifiable health information is that which can be linked to a particular person. Specifically, this information can relate to:
- The individual's present or future physical or mental health or condition;
 - The provision of health care to the individual; or,
 - The past, present, or future payment for the provision of health care to the individual.

For the purposes of this policy, all PHI is considered both sensitive information and Personal Information.

Property of MolecularMD

This document may not be used, divulged, published, or otherwise disclosed without the consent of MolecularMD.

		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 3 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

4.9 Sensitive Information: A subset of Personal Information that due to its nature has been classified by law or this policy as deserving additional privacy and security protections. Sensitive Information consists of:

- All government-issued identification numbers (including US Social Security numbers, Canadian Social Insurance numbers, driver's license numbers, and passport numbers);
- All financial account numbers (bank account numbers, credit card numbers, and other information if that information would permit access to a financial account);
- Individual medical records and biometric information, including any information on any worker, client or patient's health, disability, disease or product interests;
- Reports of individual background checks, educational transcripts, and all other data obtained from a U.S. consumer reporting agency and subject to the Fair Credit Reporting Act; and,
- Data elements revealing race, ethnicity, national origin, religion, trade union membership, sex life or sexual orientation, and criminal records or allegations of crimes.

For the purposes of this policy, all sensitive information is considered Personal Information.

4.10 Services: The functions that MolecularMD performs for, or on behalf of, a client.

4.11 USCIB: United States Council for Interational Business


5 Requirements

5.1 Duties and Responsibilities

- 5.1.1 MolecularMD shall appoint a Privacy Officer to be responsible for developing and implementing all required policies and procedures. The designated officer will be indicated on AI-0005, *Organizational Chart*.
- 5.1.2 MolecularMD must monitor and stay informed of the legal and regulatory requirements for its Processing of Personal Information and shall comply with applicable privacy or security laws and regulations.
- 5.1.3 All MolecularMD employees will promptly report any breach of confidentiality of Personal Information to their supervisor and to the Privacy Officer.
- 5.1.4 MolecularMD will promptly and thoroughly investigate allegations of any use or disclosure of Personal Information.
- 5.1.5 MolecularMD must report breaches of confidentiality of Personal Information to the relevant regulatory authorities in compliance with the regulations in effect for that jurisdiction.
- 5.1.6 The privacy officer will train all staff on appropriate procedure(s) in the event of a breach of confidentiality.

Property of MolecularMD

This document may not be used, divulged, published, or otherwise disclosed without the consent of MolecularMD.

		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 4 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

5.2 Confidentiality

- 5.2.1 MolecularMD must maintain all PI in strict confidence. MolecularMD shall make the Personal Information available only to its employees and onsite contractors who have a need to access the Personal Information in order to perform the Services. MolecularMD shall not disclose, transmit, or make available the Personal Information to third parties (including subcontractors), unless such disclosure, transmission, or making available has been explicitly authorized in the Agreement or in writing as authorized in the Agreement. In no event may MolecularMD provide Personal Information or any other client information to a third party unless that entity has agreed in writing to the terms contained within this Policy.
- 5.2.2 When MolecularMD ceases to perform Services for any client, MolecularMD shall return all PI (along with all copies and all media containing the PI) to client or shall securely destroy all PI as requested by the client. For specific records within the PI that MolecularMD is required by regulation to maintain, MolecularMD shall ensure the continued confidentiality and security of the PI and shall not actively Process the PI (other than storage) after termination of the relationship.
- 5.2.3 Any Personal Information collected or accessed in the performance of the Services contracted shall be limited to that which is necessary to perform such Services or to fulfill any legal requirements.

5.3 Client Notification


- 5.3.1 MolecularMD shall notify the client as soon as becoming aware of any of these events:
- A request for access to any PI received from an individual who is (or claims to be) the subject of the data;
 - A request for access to any PI received from any government official (including any data protection agency or law enforcement agency);
 - A inquiry, claim or complaint regarding the processing of the PI received;
 - Any breach of confidentiality of any PI related to that client; and,
 - Any other requests with respect to PI received from client employees or other third parties, other than those set forth in the agreement.

5.4 Computer Systems

- 5.4.1 MolecularMD shall have an effective process to administer access rights. The process shall include the following controls: (1) users and system resources shall only be given the access necessary to perform their required functions (FRM-0456, *Computer and Network Access Set-Up*); (2) access rights shall be updated based on personnel or system changes; and, (3) access rights shall be periodically reviewed at an appropriate frequency based on the risk to the application or system. MolecularMD shall also use effective authentication methods appropriate to the level of risk.
- 5.4.2 MolecularMD shall define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of physical penetration by malicious or unauthorized people, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.

Property of MolecularMD

This document may not be used, divulged, published, or otherwise disclosed without the consent of MolecularMD.

		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 5 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

5.4.3 MolecularMD shall secure its computer networks using multiple layers of access controls to protect against unauthorized access. Specifically: (1) group network servers, applications, data, and users into security domains; (2) establish appropriate access requirements within and between each security domain; and, (3) implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls.

5.4.4 MolecularMD shall secure access to the operating systems and applications. MolecularMD shall secure remote access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or tightly controlling access through management approvals, robust controls, logging, and monitoring access events and subsequent audits.

- Protect against the risk of malicious code by using anti-virus products on clients and servers; using an appropriate blocking strategy on the network perimeter; filtering input to applications; and creating, implementing, and training staff in appropriate computing policies and practices.
- Control and protect access to paper, film, and computer-based media to avoid loss or damage. In particular, for all media containing Sensitive Information, MolecularMD shall ensure safe and secure disposal of such media, and secure all media in transit or transmission to third parties.

5.4.5 Sensitive Information may not be stored on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks or flash drives, personal digital assistants (PDAs) or computer tapes) unless the Sensitive Information is encrypted, or the hard drive that contains the Sensitive Information on the portable computer device or media is fully encrypted.

5.5 General System Controls

5.5.1 MolecularMD shall ensure that systems are developed, acquired, and maintained with appropriate security controls.

5.5.2 MolecularMD shall identify systems and applications that warrant security event monitoring and logging, and reasonably maintain and analyze log files.


5.5.3 MolecularMD shall extend security responsibilities for outsourced operations through: (1) appropriate due diligence in service provider research and selection; and, (2) contractual assurances regarding confidentiality, security responsibilities, controls, and reporting.

5.5.4 MolecularMD shall establish a disaster recovery/business continuity plan that addresses ongoing access to the Personal Information as well as security needs for back-up sites and alternate communication networks. See POL-0013, *MolecularMD Business Continuity Planing* and SOP-0078, *Business Continuity Plan*.

5.5.5 MolecularMD shall maintain reasonable and appropriate insurance coverage in relation to the risks associated with the Processing.

Property of MolecularMD

This document may not be used, divulged, published, or otherwise disclosed without the consent of MolecularMD.

		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 6 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

6 Safe Harbor Privacy Principles


The privacy principle in this policy have been developed based on seven (7) Safe Harbor principles of notice, choice, onward transfer, access, security, data integrity and enforcement.

6.1 Notice

- 6.1.1 Where MolecularMD collects Personal Information directly from individuals in the EEA and/or Switzerland, it will inform them of the purpose for which it collects and uses the Personal Information and the types of non-agent third parties to which MolecularMD discloses or may disclose that Information and the choices and means for limiting the use and disclosure.
- 6.1.2 Where MolecularMD receives Personal Information from its clients, subsidiaries, affiliates or other entities in the EEA and/or Switzerland, it will use and disclose such information in accordance with the notices provided by such entities and the choices made by the individuals to whom such personal information relates.

6.2 Choice

- 6.2.1 Where MolecularMD collects Personal Information directly from individuals in the EEA and/or Switzerland, it will offer individuals the opportunity to choose (opt-out) whether their Personal Information is (1) to be disclosed to a non-agent third party, or (2) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.
- 6.2.2 For Sensitive Information, MolecularMD will give individuals the opportunity to affirmatively and explicitly (opt-in) consent to the disclosure of the information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.
- 6.2.3 Where MolecularMD receives Personal Information from its clients, subsidiaries, affiliates or other entities in the EEA and/or Switzerland, MolecularMD's customers are responsible, pursuant to the contractual agreements with MolecularMD, for providing choice to individuals as to whether their Personal Information may be disclosed to third parties by MolecularMD or used for a purpose that is incompatible with the purpose(s) for which the information was originally collected or subsequently authorized by the individual. MolecularMD shall inform its customers about the need to (1) provide notice to individuals about MolecularMD's privacy practices; (2) obtain consent from individuals with respect to such practices, where required by applicable law, and (3) inform individuals about the possibility that MolecularMD may disclose their Personal Information to various categories of third parties, as specified in the Onward Transfer section of this Policy.
- 6.2.4 MolecularMD does not process Personal Information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sexual orientation, except where required by law.

		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 7 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

6.3 Onward Transfer (Transfer to Third Parties)


- 6.3.1 MolecularMD shall only transfer Personal Information about individual to third party where the third party has provided assurance that it provides at least the same level of privacy protection as is required by these privacy principles.
- 6.3.2 In the event that MolecularMD transfers Personal Information to third party, it will notify individuals and provide an opt-out opportunity or obtain an opt-in if the transfer involves Sensitive Information, unless such transfers are otherwise permitted under the Safe Harbor principles.
- 6.3.3 Where MolecularMD has knowledge that third party is using or disclosing Personal Information in a manner contrary to this Policy, MolecularMD will take reasonable steps to prevent or stop the use or disclosure.

6.4 Access

- 6.4.1 Upon request, MolecularMD will grant individuals reasonable access to Personal Information that it holds about them. In addition, MolecularMD will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete.

6.5 Security

- 6.5.1 MolecularMD shall have documented and implemented appropriate operational, technical and organizational measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. MolecularMD will regularly test or otherwise monitor the effectiveness of the safeguards' controls, systems and procedures. MolecularMD will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information, and ensure that there are safeguards in place to control those risks. MolecularMD shall monitor its employees and contractors for compliance with its security program requirements. See POL-0003, *Facility Access and Security* and SOP-0133, *Software, System, & Network Access Security*.
- 6.5.2 Prior to allowing any employee or contractor to Process any Personal Information, MolecularMD shall: (1) conduct an appropriate background check of the individual; (2) require the individual to execute an enforceable confidentiality agreement (FRM-0010, *Employee Confidentiality Information Agreement*, FRM-0363, *HIPAA Confidentiality Agreement*); and, (3) provide the individual with appropriate privacy and security training.
- 6.5.3 If the Processing involves the transmission of Personal Information over a network, MolecularMD shall have implemented appropriate supplementary measures to protect the Personal Information against the specific risks presented by the Processing. Sensitive Information may only be transmitted in an encrypted format.


		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 8 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

6.6 Data Integrity

- 6.6.1 Where MolecularMD collects Personal Information directly from individuals in the EEA and/or Switzerland, MolecularMD takes reasonable steps to ensure that the Personal Information is relevant for the purposes for which the information is to be used and that the information is reliable for its intended use and is accurate, complete and current. MolecularMD depends on its customers to update and correct relevant Personal Information whenever necessary.
- 6.6.2 Where MolecularMD receives Personal Information from its clients, subsidiaries, affiliates or other entities in the EEA and/or Switzerland, MolecularMD's customers are responsible, pursuant to their contractual relationships with MolecularMD, for taking reasonable steps to ensure that the Personal Information is reliable for its intended use, accurate, complete and current.

6.7 Enforcement

- 6.7.1 MolecularMD has established annual review and audit program to monitor adherence to this policy. See SOP-0002, *Periodic Review* and SOP-0009, *Quality Assurance Auditing*. MolecularMD will investigate any breach of this policy that has been reported to MolecularMD.
- 6.7.2 In addition, MolecularMD provides a statement, at least once a year, signed by the appointed Privacy Officer or an authorized designee, verifying the adherence to the Safe Harbor Privacy Principles.
- 6.7.3 In circumstances where MolecularMD collects Personal Information directly from individuals in the EEA and/or Switzerland, individual may submit complaints concerning the processing of their Personal Information by MolecularMD directly with MolecularMD. The complaint is recorded and managed in accordance with SOP-0115, *Complaint Management*.
- 6.7.4 In circumstances where MolecularMD receives Personal Information from its clients, subsidiaries, affiliates or other entities in the EEA and/or Switzerland, individual should submit complaints concerning the processing of their Personal Information by MolecularMD in accordance with the customer's relevant dispute resolution mechanism (if available). MolecularMD will participate in the customer's dispute resolution process at the request of the individual.
- 6.7.5 MolecularMD will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Information by reference to the principles contained in this policy.
- 6.7.6 MolecularMD has chosen the EU Data Protection Authorities (EU DPAs) to serve as an independent recourse mechanism (IRM) for dispute resolution arising from collection, use, and retention of personal information transferred from EU member countries or Switzerland to companies in the United States and has subscribed to USCIB, acting as a trusted third party on behalf of the European Union (EU) Data Protection Authorities.

		Title: Privacy Policy	
		Document Number: POL-0024	Revision: 004
Policy	Page 9 of 9	Change Notice: CN-0910	Effective Date: 01Feb2016

7 Contact Information

Questions or comments regarding this Policy shall be submitted to MolecularMD using any of the contact information below.

By mail: MolecularMD

1341 SW Custer Drive

Portland, OR 97219

By Tel: 503-459-4974

By Fax: 503-459-4976

By Email: clientservices@molecularmd.com

8 Document History

Rev	Author	Description of Change
001	Kevin Hawkins	Initial release of document.
002	MaiLy Le	Incorporated Safe Harbor Privacy Principles. Added section 6 & 7.
003	Jessica Horowitz	Added reference to POL-0017, <i>Organizational Chart</i> in section 5 and added step 5.1.6. Added section 6.7.6, and updated Section 4, <i>Definitions, Acronyms, Abbreviations</i> as appropriate.
004	Jessica Horowitz	Updated Section 1, <i>Purpose</i> to comply with U.S.-EU Safe Harbor and U.S.-Swiss Safe Harbor requirements. Updated Section 3, <i>Related Documents</i> to update titles for POL-0013 and SOP-0078 and remove reference to the superseded POL-0004. Added EEA to Section 4, <i>Definitions, Acronyms, Abbreviations</i> . Removed reference to POL-0017, <i>Organizational Chart</i> throughout document. Added reference to AI-0005, <i>Organizational Chart</i> , to Section 3 and Step 5.1.1 Updated Step 5.5.4 to remove reference to superseded POL-0004 and list the updated document titles for POL-0013 and SOP-0078. Added reference to Switzerland in Step 6.7.6.