CONFIDENTIALITY AND INFORMATION ACCESS AGREEMENT

Summary

MolecularMatch ("the Company") is dedicated to safeguarding and maintaining the confidentiality, integrity, and availability of ePHI, employee, and organizational information (collectively "Confidential Information"). ePHI refers to information includes protected health information that is any personal, employment-related, or medical information relating to a patient's treatment or payment that is created and/or stored in any information system. The confidentiality, integrity, and availability of protected health information must be maintained at all times.

This Confidentiality and Information Access Agreement ("Agreement") is required to be read, signed, and complied with by all users that access any of the organization's information systems as a condition of access to any information system. The information system user signing this Agreement may only access, use, and disclose Confidential Information in any medium as needed to perform his/her job responsibilities as allowed by law, organization policies and procedures, and/or as agreed upon between said user and the Company.

1. I understand and agree that I must safeguard and maintain the confidentiality, integrity, and availability of all Confidential Information I use, disclose, and/or access at all times, whether or not I am at work and regardless of how it was accessed.	*7. I understand that access to any Information Systems including Email and Internet are intended for business usage.*
2. I will only access, use, and/or disclose the minimum necessary Confidential Information needed to perform my assigned duties and disclose it to other individuals/organizations who need it to perform their assigned duties or as allowed by law. Protected health information is specifically protected by law from further disclosures without prior authorization.	*8. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved privacy and security standards.*
3. I will not access my own, or my family's, record in any information system without prior Authorization (unless required to perform your job responsibilities).	*9. I will only access or use the systems or devices that I am being authorized to access and agree not to demonstrate the operation or function of any information systems or devices to unauthorized individuals.*
4. I will not disclose any Confidential Information with others who do not have a need to know it.	*10. I will never use tools or techniques to break/exploit security measures.*
5. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.	*11. I will not use any information system to transmit, retrieve, nor store any communications consisting of discriminatory, harassing, obscene, solicitation, or criminal information.*
6. I will not download any Confidential Information off any information system to store or use it on any other system or removable storage devices such as removable USB flash discs, except in situations whereby explicit approval to do so has been granted with prior review by the Security Officer & Privacy Officer. If I received this approval to download data I will assume sole and absolute responsibility to manage and protect it based upon standards listed in this Agreement and according to the law.	*12. I understand that I have neither ownership interest nor expectation of privacy in any information accessed or created by me during my relationship with the Company. Information may be audited, logged, accessed, reviewed, and otherwise utilized that is stored on or passing through any information system. This may be done for many reasons, including maintaining the confidentiality, security, and availability of Confidential Information.*

13. I understand that my User Login ID(s), password(s) are used to control access to information systems and an electronic signature(s) is the equivalent to my legal signature. I will not disclose them to anyone nor allow anyone to access any information system using my User Login ID(s) and password(s) for any reason.	*16. I will immediately report to the Privacy officer any activity that violates this agreement, Confidential Information laws, or any other incident that could have any adverse impact on Confidential Information.*
14. I will only use my officially assigned, personal User Login ID(s) and password(s).	*17. Upon completion and/or termination of access to any information system, the Human Resources department (or other designated department) will the Security Officer to delete users access to information systems/applications.*
15. I will immediately notify the Privacy Officer if my password has been seen, disclosed, or otherwise compromised.	*18. I affirm that I will maintain the confidentiality, integrity, and availability of all Confidential Information even after termination, completion, cancellation, expiration, or other conclusion of access to any information system.*
19. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment or business relationship, suspension and loss of privileges, termination of authorization to work as well as legal actions.	

Refer any questions related to this Agreement to the Security Officer or the Privacy Officer.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it. Access to information systems may be denied if this Agreement is not returned signed and dated.

_____ _____

Signature *Date*

Please return this completed Agreement to: Privacy Officer