Personal Identity Information (PII) Security, Notification and Confidentiality Policy

Scope of this Privacy Policy

This Privacy Policy is applicable to any PII or information that you may provide us or is collected from you via the www.andorhealth.com website. This includes any application or websites which are added to this Privacy Policy ("services"). By using any of these Services, or voluntarily providing your PII to us, you consent to our use and collection of this data as set in this Privacy Policy. If you do not agree, please do not provide us with any information and do not use our Services.

The scope of this Privacy Policy is only applicable to PII collected or submitted through the Services and does not include any information that may be collected by Andor Health through other means. This policy also does not apply to PII collected by third party services, applications, or website that are liked to or accessible from the Sites. The PII or other information collected by third parties (such as Microsoft Teams), is subject to their own privacy policies and under no circumstances is the Company responsible or liable for the third party's compliance.

Purpose of this Policy

Andor Health recognizes its need to maintain the confidentiality of Personal Identity Information (PII) and understands that such information is unique to each individual. The PII covered by this policy may come from various types of individuals performing tasks on behalf of the company and includes employees, applicants, independent contractors and any PII maintained on its customer base. The scope of this policy is intended to be comprehensive and will include company requirements for the security and protection of such information throughout the company and its approved vendors both on and off work premises. Departments named in this policy have delegated authority for developing and implementing procedural guidance for ensuring that their departmental responsibilities under this policy are communicated and enforced.

Key Elements of the Policy

Personal Identity Information (PII): Unique personal identification numbers or data, including:

- Social Security Numbers (or their equivalent issued by governmental entities outside the United States).
- Taxpayer Identification Numbers (or their equivalent issued by governmental revenue entities outside the United States).
- Employer Identification Numbers (or their equivalent issued by government entities outside the United States).
- State or foreign drivers license numbers.
- Date(s) of birth.
- Corporate or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records.

PII may reside in hard copy or electronic records; both forms of PII fall within the scope of this policy.

Vendors: Individual(s) or companies that have been approved by the Contracts Department as a recipient of organizational PII and from which the Contracts Department has received certification of their data protection practices conformance with the requirements of this policy. Vendors include all external providers of services to the company and include proposed vendors. No PII information can be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information.

Third party applications and services: This Privacy Policy does not encompass or apply to any information collected through third party services. The information received by any third parties is subject to their privacy terms and policies. The company is not liable for the third party's adherence or compliance to the privacy policy. This includes any links to third party websites. The terms listed in this Privacy Policy generally apply to "ThinkAndor," "AndorNow," and the website noted in this Privacy Policy. To note, the Andor Health Website and application include functionalities provided by Microsoft Teams.

PII Retention: Andor Health understands the importance of minimizing the amount of PII data it maintains and retains such PII only as long as necessary. A joint task force comprising members of the Legal, Finance, IT, Contracts and Human Resources departments maintains organizational record retention procedures, which dictate the length of data retention and data destruction methods for both hard copy and electronic records.

PII Training: All new hires entering the company who may have access to PII are provided with introductory training regarding the provisions of this policy, a copy of this policy and implementing procedures for the department to which they are assigned. Employees in positions with regular ongoing access to PII or those transferred into such positions are provided with training reinforcing this policy and procedures for the maintenance of PII data and shall receive annual training regarding the security and protection of PII data and company proprietary data.

PII Audit(s): Andor Health conducts audits of PII information maintained by the company in conjunction with fiscal year closing activities to ensure that this policy remains strictly enforced and to ascertain the necessity for the continued retention of PII information. Where the need no longer exists, PII information will be destroyed in accordance with protocols for destruction of such records and logs maintained for the dates of destruction. The audits are conducted by Finance, IT, Contracts and Human Resources departments under the auspices of the Legal department.

Data Breaches/Notification: Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, the company will notify all affected individuals whose PII data may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible and in no event be later than the commencement of the payroll period after which the breach was discovered.

The Legal department will handle breach notifications(s) to all governmental agencies to whom such notice must be provided in accordance with time frames specified under these laws. Notices to affected individuals will be communicated by Human Resources after consultation with the Legal department and within the time frame specified under the appropriate law(s).

Data Access: Andor Health maintains multiple IT systems where PII data may reside; thus, user access to such IT systems is the responsibility of the IT department. The IT department has created internal controls for such systems to establish legitimate access for users of data, and access shall be limited to those approved by IT. Any change in vendor status or the termination of an employee or independent contractor with access will immediately result in the termination of the user's access to all systems where the PII may reside.

Data Transmission and Transportation

1. Company Premises Access to PII: The Finance, Human Resources and IT departments have defined responsibilities for on-site access of data that may include access to PII; IT has the oversight responsibility for all electronic records and data access capabilities. Finance and Human Resources have the operational responsibility for designating initial access and termination of access for individual users within their organizations and providing timely notice to IT.

2. Vendors: Andor Health may share data with vendors who have a business need to have PII data. Where such inter-company sharing of data is required, the IT department is responsible for creating and maintaining data encryption and protection standards to safeguard all PII data that resides in the databases provided to vendors. Approved vendor lists will be maintained by the Contracts department, and Contracts has responsibility to notify IT of any changes to vendor status with the company.

3. Portable Storage Devices: Andor Health reserves the right to restrict PII data it maintains in the workplace. In the course of doing business, PII data may also be downloaded to laptops or other computing storage devices to facilitate company business. To protect such data, the company will also require that any such devices use IT department-approved encryption and security protection software while such devices are in use on or off company premises. The IT department has responsibility for

maintaining data encryption and data protection standards to safeguard PII data that resides on these portable storage devices.

4. Off-Site Access to PII: Andor Health understands that employees may need to access PII while off site or on business travel, and access to such data shall not be prohibited, subject to the provision that the data to be accessed is minimized to the degree possible to meet business needs and that such data shall reside only on assigned laptops/approved storage devices that have been secured in advance by the IT department.

Regulatory Requirements: It is the policy of the company to comply with any international, federal or state statute and reporting regulations. Andor Health has delegated the responsibility for maintaining PII security provisions to the departments noted in this policy. Andor Health's Legal department shall be the sole entity named to oversee all regulatory reporting compliance issues. If any provision of this policy conflicts with a statutory requirement of international, federal or state law governing PII, the policy provision(s) that conflict shall be superseded. All inquiries can be directed to compliance.inquiries@andorhealth.com.

Employee Hotline: If an employee has reason to believe that his or her PII (please refer to what constitutes PII) data security has been breached or that company representative(s) are not adhering to the provisions of this policy, an employee should contact an HR representative at the employee's location. HR contact information: hr@andorhealth.com.

Confirmation of Confidentiality: All company employees must maintain the confidentiality of PII as well as company proprietary data to which they may have access and understand that that such PII is to be restricted to only those with a business need to know. Employees with ongoing access to such data will sign acknowledgement reminders annually attesting to their understanding of this company requirement.

Violations of PII Policies and Procedures: Andor Health views the protection of PII data to be of the utmost importance. Infractions of this policy or its procedures will result in disciplinary actions under the company's discipline policy and may include suspension or termination in the case of severe or repeat violations. PII violations and disciplinary actions are incorporated in the company's PII onboarding and refresher training to reinforce the company's continuing commitment to ensuring that this data is protected by the highest standards.