ELECTRONIC ACCESS AGREEMENT

Name (Please Print): _____ UVA Computing ID: _____

Employer/Sponsor: Medical Center | UVa Physicians Group | Academic Division | UVA-Wise | University-Associated Organization

Department:_____

The following apply to any and all access or use of UVA's information technology (IT) resources.

1. I will not obtain or attempt to obtain unauthorized access to UVA's IT resources *(defined below)*, circumvent or attempt to circumvent security controls on UVA's IT resources, nor allow unauthorized users access to UVA's IT resources at any time, whether during my period of employment or following my separation from the University.

2. I will not divulge or share my passwords, PINs, private keys, hardware tokens, or similar authentication elements ("electronic credentials") to or with other individuals, or allow others to use an account that I have logged into using my electronic credential. I acknowledge that the combination of my computing ID and electronic credential (or use of a hardware token) is considered equal to my electronic signature. I understand that I will be held responsible for the consequences of any misuse occurring under my electronic credential due to any action or neglect on my part.

3. I will not use another person's electronic credential. If I have reason to believe that my electronic credential, or those of another individual have been compromised or are being used by a person other than the individual to whom they were issued, I will immediately report it to the appropriate Information Security office in the UVA-Wise, UVA Academic Division, UVA Medical Center, or UVA Physicians Group.

4. I will immediately report any suspected breaches of confidentiality of highly sensitive data *(defined below)*, including patient information, to the appropriate Information Security and Compliance offices.

5. I agree to access or alter only the information for which I have responsibility or authorization, and not to view information that I have no need to see as part of my responsibilities. Access to or use of any UVA IT resource and the data it contains (that was not already intentionally made public) for my own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity is strictly forbidden.

6. I will respect the privacy and confidentiality of individuals to whose information I have been given access. I will not view or disclose that information except as required by my responsibilities and as allowed by UVA-Wise, UVA Academic Division, UVA Medical Center, and UVA Physicians Group policies and applicable law. I will not use UVA IT resources to access or disclose the address, email address or phone number of a student unless I have a legitimate educational interest *(defined below)* in that information.

7. I understand that the transactions processed with my electronic access may be audited, and appropriate action will be taken if improper uses are detected.

8. I agree to follow the privacy, security, and other computing policies, standards, and procedures established by UVA-Wise, UVA Academic Division, UVA Medical Center, and UVA Physicians Group, as well as all local, state, and federal laws, including security and privacy laws and regulations, that apply to the use of my electronic credential and to the UVA IT resources I access.

9. I understand these concepts apply to all UVA IT resources, both fixed and mobile devices (such as, but not limited to desktop computers, laptops, tablets, smartphones and text-enabled pagers). I also agree to safeguard the information I access and the devices assigned to me and report any losses promptly to the appropriate Information Security office.

My signature below indicates that I have read, understand, and agree to abide by these requirements and applicable policies. Failure to do so may result in the limitation or revocation of my access to UVA IT resources and/or disciplinary actions, up to and including termination or expulsion in accordance with relevant University policies.

_____ _____

Signature **Date**

Glossary:

Highly sensitive data (HSD), as defined in the UVA Policy IRM-003: Data Protection of University Information, are: data that require restrictions on access under the law or that may be protected from release in accordance with applicable law or regulation, such as Virginia Code § 18.2-186.6. Breach of Personal Information Notification. Highly Sensitive data (HSD) currently include personal information that can lead to identity theft. HSD also includes health information that reveals an individual's health condition and/or medical history. Specific examples include, but are not limited to:

- *Any store or file of passwords or user-ids and passwords* on any multi-user system or computer.
- *Personal information that, if exposed, can lead to identity theft.* This may include a personal identifier (e.g., name, date of birth) as well as one of the following elements:
    - Social security number;
    - Driver's license number or state identification card number issued in lieu of a driver's license number;
    - Passport number;
    - Financial account number in combination with any required security code, access code, or password that would permit access to a financial account;
    - Credit card or debit card number, including any cardholder data in any form on a payment card: or
    - Military Identification Number.

Also considered HSD are any form of personally identifying information in combination with social security number (SSN), driver's license number, passport number, financial account number and required security code, and/or military ID number. For example, computing ID and driver's license number, or home address and SSN.

Note that credit card numbers can never be stored either alone or in combination with any other identifiers.

- *Health information is any information that, if exposed, can reveal an individual's health condition and/or history of health services use, including information defined by* Health Insurance Portability and Accountability Act *(HIPAA) as protected health information (PHI).*
- **Cardholder Data (CHD):** Primary cardholder account number that identifies the issuer and a particular cardholder account, which can include cardholder name, expiration date and/or service code.

Information Technology (IT) Resources: All resources owned, leased, managed, controlled, or contracted by the University involving networking, computing, electronic communication, and the management and storage of electronic data including, but not limited to:

- Networks (virtual and physical), networking equipment, and associated wiring including, but not limited to: gateways, routers, switches, wireless access points, concentrators, firewalls, and Internet-protocol telephony devices;
- Electronic devices containing computer processors including, but not limited to: computers, laptops, desktops, servers (virtual or physical), smart phones, tablets, digital assistants, printers, copiers, network-aware devices with embedded electronic systems (i.e., "Internet of things"), and supervisory control and data acquisition (SCADA) and industrial control systems;
- Electronic data storage devices including, but not limited to: internal and external storage devices (e.g., solid state and hard drives, USB thumb drives, Bluetooth connected storage devices), magnetic tapes, diskettes, CDs, DVDs;
- Software including, but not limited to: applications, databases, content management systems, web services, and print services;
- Electronic data in transmission and at rest;
- Network and communications access and associated privileges; and
- Account access and associated privileges to any other IT resource.

Legitimate educational interest: refers to the need of school officials, including those performing the functions described below, to access specific Education Records in the course of performing their duties for UVA.

School officials are those individuals who engage in the instructional, supervisory, advisory, administrative, governance, public safety, research, and support functions of UVA. They need not necessarily be paid employees of UVA. School officials include but are not limited to:

- Those UVA students who, pursuant to their duties as officers in officially recognized honor societies, periodicals, and other activities that recognize or encourage superior academic achievement, require personally identifiable information (e.g., grades) from students' education records to determine the satisfaction of specified eligibility requirements;
- Those UVA students who, pursuant to their duties as members of official UVA committees (e.g., scholarship committees), require personally identifiable information from Education Records;
- Those UVA students who, pursuant to the authority granted by the Board of Visitors under the terms of the Honor System and the University Judiciary System, require personally identifiable information from Education Records to investigate, adjudicate, or advise students involved in an alleged violation of the Honor Code or the Standards of Conduct;
- Those persons, companies, or agencies under UVA's direct control, with whom UVA has contracted to provide services that UVA itself would provide otherwise.

From UVa Policy: STU-002 (https://uvapolicy.virginia.edu/policy/STU-002)