BON SECOURS MERCY HEALTH

Confidentiality and Security Agreement

Bon Secours Mercy Health (BSMH) has a legal and ethical responsibility to safeguard the privacy of all patients, residents, workforce members and clients and to protect the confidentiality of their Protected Health Information (PHI), Personal Health Information, Personal Data, Personally Identifiable Information (PII), and Payment Card Information (PCI). BSMH must also protect the integrity and confidentiality of organizational information and information systems that may include, but are not limited to, fiscal, research, internal reporting, strategic planning, communications, and computer systems from any source or in any form including, without limitation, paper, magnetic or optical media, conversations, electronic, and film.

For the purpose of this Agreement, all such information is referred to as "Sensitive Data." This includes:

- "Protected Health Information (PHI)" as defined by the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations.
- "Personal Data" as defined by the Philippines Data Privacy Act of 2012 (Republic Act No. 10173, DPA), which includes personal information, sensitive personal information, and privileged information.
- "Personally Identifiable Information (PII)" as defined under U.S. state and federal privacy laws, which includes data that can directly or indirectly identify an individual (e.g., SSN, financial account information, driver's license numbers, dates of birth, employee, or student records).
- "Payment Card Information (PCI)", which includes cardholder data and sensitive authentication data, as defined by the Payment Card Industry Data Security Standard (PCI DSS).

When handling PHI or Personal Data of individuals located in or originating from the Philippines, BSMH and its workforce members must comply with:

- The HIPAA Privacy, Security, and Breach Notification Rules and all other applicable U.S. federal and state laws,
- The Philippines DPA, its Implementing Rules and Regulations, and applicable issuances of the National Privacy Commission (NPC),
- PCI DSS standards for payment card information, and
- Other applicable U.S. state, federal, and international privacy, and data protection laws.

I **UNDERSTAND AND HEREBY AGREE THAT:**

1. During my employment / affiliation with BSMH, I understand that I may have access and exposure to Sensitive Data.
2. I will access and / or use Sensitive Data only as necessary to perform my job-related duties and in accordance with BSMH's policies and procedures.
3. My User-ID and password are confidential, and in certain circumstances may be equivalent to my **LEGAL SIGNATURE**, and I will not disclose them to anyone.
4. I will not copy, release, sell, loan, alter, or destroy any Sensitive Data except as properly authorized by law or BSMH policy.
5. I will not discuss Sensitive Data so that it can be overheard by unauthorized persons. It is not acceptable to discuss information that can identify a patient or data subject in a public area even if the name is not used.
6. I will only access and / or use systems or devices I am authorized to access and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
7. I have no expectation of privacy when using BSMH information systems. BSMH has the right to log, access, review, and otherwise use information stored on or passing through its systems, including e-mail.
8. I will never connect to unauthorized networks through BSMH's systems or devices.
9. I will practice secure electronic communications by transmitting Sensitive Data in accordance with approved BSMH security standards and applicable data protection laws and regulations.
10. I will practice good workstation security measures such as never leaving a terminal unattended while logged in to an application, locking up removable media when not in use, using screen savers with activated passwords appropriately, and positioning screens away from public view.
11. I will:
    a. Use only my assigned User-ID and password.
    b. Use only approved licensed software.
    c. Use a device with virus protection software.

d. Not attempt to learn or use another's User-ID and password.
e. Not store Sensitive Data in a manner inconsistent with BSMH policy, standards or applicable data protection laws and regulations.

12. I will disclose Sensitive Data only to authorized individuals with a need to know that information in connection with the performance of their job function or professional duties.
13. Unauthorized or improper use of BSMH's information systems and / or Sensitive Data is strictly prohibited and may not be covered by BSMH's insurance or my personal professional malpractice insurance. **Any such violation may subject me to personal liability, as well as sanctions for violation of U.S. state and federal law, the DPA, or other applicable laws or regulations.**
14. I will notify my manager, BSMH Privacy Officer, IS Security, or other appropriate Information Services personnel if my password has been seen, disclosed, or otherwise compromised.
15. Upon termination of my employment / affiliation / association with BSMH, I will immediately return or destroy, as appropriate, any Sensitive Data in my possession.
16. Violation of this Agreement may result in disciplinary action, up to and including civil or criminal action, termination of employment / affiliation / association with BSMH, and suspension and / or loss of medical staff privileges in accordance with BSMH's policies.
17. My obligations under this Agreement will continue after termination of employment / affiliation / association with BSMH.

By signing this document, I acknowledge that I have read this Agreement, and I agree to comply with all the terms and conditions stated above.

Signature _____ Date _____

Printed Name _____

Non-BSMH Organization Name _____