POLICY & PROCEDURE SUBJECT: Appropriate Use of Patient Information by Staff CC *IHN* DEPT: CORPORATE COMPLIANCE	Page 1 of 2 EFFECTIVE Date: 06/11/2013 REVIEW Date: 02/07/2020

I. Policy

Inspira is committed to safeguarding the privacy of patient information and maintaining the integrity of all information systems containing patient information. It is the responsibility of Inspira Health staff, physicians, volunteers and vendors and any other individual with access to patient information to ensure the confidentiality of any and all patient information.

II. Scope

Patient Information is defined as any information that individually identifies a patient or has the potential to identify a patient. Patient information may or may not include medical, financial or demographic information. Including but not limited to medical records, billing documentation lab reports, or images of a patient are considered confidential information and are subject to Confidentiality HR.15 *IHN*

Use and disclosure of patient information must be for treatment, payment or healthcare operations as outlined in Permitted Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations CC.19 *IHN*

Any purpose not outlined in this or other Inspira policies will be considered an improper use of confidential information and will be subject to disciplinary action.

Access to Inspira Information Systems containing patient information is granted for work related purposes. Employees may only access information including hardcopy or electronic files, medical records and information system programs to perform work related duties.

Employees are required to save files including those that include confidential information to the personal folders ex*. H Drive* rather than local computer folders *C Drive* or *My Documents* to ensure data can be properly accessed and backed up.

Employees are required to safeguard all passwords and login information. Login information is considered confidential and should not be shared with others. All activity attributed to an Employee's user id will be attributed to the Employee. Employees must log off systems when they are not using them to avoid use by others. Failure to do so may be the basis for disciplinary action.

The following is strictly prohibited:

Participation in viewing, accessing, downloading, uploading, photographing, using or disclosing confidential information for any purpose other than carrying out job-related responsibilities.

Examples:

Accessing your own information; family members; another Inspira Employee or any person for whom an Employee may act as Personal Representative e*x. Power of Attorney, Parent/Legal Guardian or Healthcare Proxy;*

Removing patient information including printed materials or electronic from any Inspira location without obtaining permission from a Manager or Director. Permission shall be granted at the Manager's

discretion with appropriate precautions of minimum necessary data elements and use of encrypted portable devices or media.

Downloading patient information to unencrypted devices such as thumb drives, flash drives or any other removable media.

Uploading or placing patient information on non-approved websites or software including social media or shared internet sites.

Transmission of patient information to non-Inspira email without proper safeguards such as encryption. Encryption instructions can be found on the intranet. Internal email containing patient information between Inspira staff is permissible. Email and Communication Systems IS-054

Staff obligation to report

Employees must report any incident involving improper use or disclosure of patient information ex. misdirected facsimiles, lost or stolen devices containing patient information or improper access of patient information to the Corporate Compliance or Information Systems Departments immediately. Options for reporting may include contacting Corporate Compliance staff; communicating concerns to the Corporate Compliance Hotline; and forwarding an email to the Corporate Compliance Department at mailto:compliance@ihn.org .

Mitigation of Improper Disclosures CC.15 *IHN*

Disciplinary Action

Employees who inappropriately use patient information or violate HIPAA law may be subject to disciplinary action, up to and including termination.