Patient Confidentiality in the Practitioner's Office Policy

BlueShield of Northeastern New York

Last Reviewed: June 20, 2018

Last Revised: June 20, 2018

Policy:

A patient confidentiality policy for practitioners' offices, including behavioral health practitioners, ensures privacy of the health information of BlueShield of Northeastern New York members. These guidelines are supported by the National Committee for Quality Assurance (NCQA) Standards and Guidelines for Health Plan Accreditation. The guidelines are as follows:

- Staff should avoid discussing patient cases where they can be overheard by others.
- When voices can be heard easily through exam room walls, adding soundproof panels or playing soft music can help, but is not required.
- Arrange office space to allow privacy for your patients who are paying bills and making appointments.
- Ensure computer screens that contain patient information are protected from general view.
- Ensure all patient care is provided out of sight from other patients (weighing, lab draws, etc.).
- Avoid listing patient telephone number or reason for visit on the sign-in sheet.
- Office staff receives periodic training in member information confidentiality. Have an office confidentiality policy for staff to read and sign.
- Ask your patients to sign a HIPAA-compliant Authorization to Release Information form prior to releasing medical records to anyone (other physicians, Department of Health, etc.).
- Information containing HIV/AIDS status or substance abuse must have a **separate release form** stating the practitioner has the permission of the patient to send that information.
- BlueShield may obtain its members' medical records, as all members sign an agreement regarding this upon enrollment with BlueShield. Providers are not required to release a patient's HIV and substance abuse information to BlueShield without patient authorization.
- Set in place a protocol for sending and receiving confidential information via fax.
- Ensure medical record files are organized and stored in a secure manner that allows for easy retrieval by authorized personnel only. Records should not be accessible to the public.
- Ensure electronic medical records are secured by individual password for each practitioner/staff member.
- Keep all patient medical records out of the view of others.

Adherence to this policy is evaluated during the practitioner office compliance attestation process or onsite review and through evaluation of member complaints.

11282 HCQI 1700 NENY 2018