Blue Cross and Blue Shield of Louisiana
HMO Louisiana
Southern National Life

Member Data Protection Statement

At Blue Cross and Blue Shield of Louisiana, our mission is to improve the health and lives of Louisianians – including how we store, use and protect our members' data. Blue Cross has strong processes in place, which all of our employees must follow to protect members' data in all forms (spoken, written and/or electronic).

Blue Cross approaches members' data protection from three perspectives – physical security, cybersecurity and privacy. Blue Cross recruits, hires and trains qualified staff who work together to safely store our members' information and make sure all employees are following the laws and regulations that protect it.

Blue Cross has extensive policies and procedures that outline the security and privacy standards and responsibilities for protecting members' data. Employees are trained on Blue Cross data protection protocols as soon as they start working here, and all employees have refresher training at least once a year.

Blue Cross does not give every employee access to members' information, and not all access is the same. How much member information any Blue Cross employee can access depends on his/her job and role within the company. Employees can only get to the information they need to do their jobs and not anything else. For example, a Customer Service adviser who needs member information to answer calls is able to see those records, but a business analyst working on internal projects would not need this access.

Spoken Data
Before Blue Cross employees give information over the phone or in person, they take steps to authenticate the identities of the people requesting information. This is to make sure the people calling are really who they say they are and that they have the right to request that information. Blue Cross has a process for our members to let us know whom they want to be an authorized delegate or legal representative. That means you are giving permission for them to contact Blue Cross and ask for information on your behalf.

Written Data
Blue Cross has strong privacy protection rules for paper documents. Employees are required to keep records in a safe place where they cannot be seen, for example in a locked file cabinet instead of lying on a desk. Blue Cross requires employees to go through their computers and securely destroy electronic files that are no longer needed. This prevents the information in these records from being stolen or accessed by the wrong people.

Electronic Data
Blue Cross IT staff uses the latest technology to keep electronic information secure by encrypting it within internal systems so that no one can get to it from outside the system. The IT staff members have processes in place to detect and prevent hackers from getting to our technical systems and monitor how employees access and use information within the organization.

If you have questions about how Blue Cross uses, stores or protects members' data, call our Information Governance Office at (225) 298-1751.

12PR0095 05/18