

McLaren Health Care Corporation
ACCEPTABLE USE AND CONFIDENTIALITY ACKNOWLEDGEMENT FORM

“Confidential and Proprietary Information” includes information relating to:

- A. Any individuals’ Protected Health Information (PHI), which is information that identifies an individual (name, social security number, account number, etc.) and is created or received by a health care provider, health plan, or healthcare clearinghouse, is transmitted or maintained in any medium (i.e. electronic, medical record, paper, oral), and relates to the past, present or future physical or mental health condition, or payment for the provision of care (including medical records, conversations, admitting information, and patient financial information);
- B. Employees (including medical records, compensation, benefits, employment records, and disciplinary actions);
- C. McLaren Health Care Corporation’s or subsidiary specific information (including financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs and technology and source code); and
- D. Proprietary third-party information (including computer programs and technology, client or vendor information and source code).

I understand and acknowledge:

- 1. As a member of the workforce (employees, physicians, contracted personnel, volunteers, students, etc.) I may learn of or have access to Confidential and Proprietary Information through computer systems (including, but not limited to patient care information systems, other clinical and financial information systems, the longitudinal patient record, and the actuarial and claims systems) or through my employment.
- 2. I understand it is my responsibility to use Confidential and Proprietary Information only as minimally necessary to perform my legitimate job duties, as well as safeguard and limit access to any Protected Health Information in *any medium* (including written, oral or electronic formats).
- 3. I understand it is my responsibility to safeguard my access code and I will not share my access code or other authorization for access to Confidential and Proprietary Information.
- 4. I understand it is my responsibility to protect any and all Confidential and Proprietary Information obtained as a member of the workforce even after my employment or association has ended with MHCC or a subsidiary of the corporation.
- 5. I understand the organization may routinely monitor and audit my E-mail and internet use, and access to information regarding, but not limited to, employees, physicians and patients, their relatives, public figures, and VIPs for appropriateness of use and access to such information as it relates to my legitimate duties.
- 6. I understand it is my responsibility to sign off the computer when I leave the computer system.
- 7. I understand that I am responsible for all activity logged under my password. I understand that I must log off before another user may use the computer.
- 8. I understand it is my responsibility to use the E-mail system, internet, and all electronic devices and media, including those I may personally own and use for work or to access work documents and E-mail on, in ways consistent with the Technology and Resources policy.
- 9. I understand it is my responsibility to notify my supervisor or the Privacy/Security Officer immediately if I suspect or learn of any privacy or security breach, e.g., that my access code, other authorization for access to Confidential and Proprietary Information has been misused or disclosed without proper authorization. I understand the purpose of this notification is to protect confidentiality and that my unique information systems access code(s) may be changed.
- 10. I understand that my employer may, at any time, revoke my access code or other authorization for access to Confidential and Proprietary Information.
- 11. I understand that violation of my duties as discussed above may independently constitute a violation of applicable criminal/civil laws.
- 12. I acknowledge that I have received training and understand concepts regarding confidentiality, privacy, and security as they relate to the Health Insurance Portability and Accountability Act (HIPAA), and was given the opportunity to ask questions.