





POLICY & PROCEDURE

Title: ELECTRONIC INFORMED CONSENT IN CLINICAL RESEARCH	Policy Number: BC-CR303
Sponsored by: BayCare Sponsored Programs & Research and BayCare Institutional Review Board	Issued for: All BayCare, including without limitation: Bartow Regional Medical Center Mease Countryside Hospital Mease Dunedin Hospital Morton Plant Hospital Morton Plant North Bay Hospital South Florida Baptist Hospital St. Anthony's Hospital St. Joseph's Hospital Winter Haven Hospital
Original Issue: 2/17/2021 Review Dates: 11/18/2020 Revision Date:	Approved by: Edward Rafalski Signature: <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <small>DocuSigned by:</small>  <small>1C605CA03849475...</small> </div> Approved by: Dr. Mark Vaaler Signature: 

PURPOSE:

The purpose of this policy is to outline the process and responsibility for obtaining electronic informed consent (eIC) from an individual for participation in a research study.

DEFINITIONS:

Electronic Informed Consent (eIC) means the use of electronic systems and processes that may employ multiple electronic media, including text, graphics, audio, video, podcasts, and websites to convey information related to the study and to obtain and document informed consent.

Electronic Signature (eSIG) means the electronic process attached to a record and adopted by a person with the intent to sign the record.

Electronic System means the electronic technology selected for the electronic informed consent process.

Identification Codes / Passwords means those methods or combination of methods used by a genuine owner and not able to be reused by, or reassigned to, anyone else.

Informed Consent means providing a potential subject with adequate information to allow for an informed decision about participation in a study, facilitating the potential subject's comprehension of the information, providing adequate opportunity for the potential subject to ask questions and to consider whether to participate, obtaining the potential subject's voluntary agreement to participate, and continuing to provide information as the study progresses or as the subject or situation requires.

Institutional Review Board (IRB) means the board formally designated by BayCare Health System (BayCare) to review and approve the initiation of studies, and to conduct periodic review of studies.

Principal Investigator (PI) means the individual responsible for ensuring that legally effective informed consent is obtained before a subject takes part in a study.

Person Explaining Consent (PEC) means the person who is authorized by the Principal Investigator to obtain consent.

Subject means the person who is giving consent to participate in a research study or his/her legally authorized representative (LAR).

POLICY:

The PI, PEC or CRC may obtain informed consent to participate in a research study by either paper-based informed consent or eIC. The PI, PEC or clinical research coordinator (CRC) shall confirm whether a Subject prefers the option of using paper-based or eIC, completely or partially, throughout the study. The PI, PEC or CRC shall be responsible for documenting the Subject's preference in the Subject's medical record; however, the PI is ultimately responsible for ensuring that the process selected by the Subject is adhered to.

If a Subject selects to use eIC, this policy shall apply, in addition to the **Informed Consent Process for Research Studies Policy (BC-RES-105)**. The eIC shall contain all of the elements of informed consent required by the U.S. Department of Health and Human Services (HHS) and/or the Food & Drug Administration (FDA) (45 C.F.R. 46.116 and 21 CFR 50.25). The PIs are responsible for the informed consent process and shall send the eIC for review and approval by the IRB, prior to utilizing it. The IRB shall be responsible for: (1) reviewing and approving, as appropriate, the eIC and any amendments to the eIC; and (2) maintaining copies of all approved eIC forms, including any content linked to the eIC. Any eIC shall be obtained through the use of an Electronic System that satisfies the requirements detailed in **Exhibit A, "Electronic System Requirements for Electronic Informed Consent."**

PROCEDURE:

1. Obtaining the eIC

- a. Before obtaining the Subject's eIC, the Electronic System shall verify the identity of the Subject, in accordance with Exhibit A, "Electronic System Requirements for Electronic Informed Consent."

Consent of Children: If the study involves children, the parent may initially document the child's assent; however, in such a situation, the PI shall verify the child's identity when he/she sees the child in person.

- b. The PI, PEC or CRC shall ensure the Subject is provided with the information that a reasonable person would want to have in order to make an informed decision about whether to participate in the research study, and shall allow him/her an opportunity to ask questions.

Video Conferencing: If used, both the PI, PEC or CRC and Subject shall find a private location to have the discussion, to ensure privacy and confidentiality.

- c. A HIPAA authorization to use or disclose Protected Health Information for research purposes may be obtained electronically if the individual's signature is a valid electronic signature under applicable law.

2. Documentation of the eIC

- a. A copy of the eIC shall be provided to the Subject, which shall include the Subject's signature and the date when the eIC is signed. It shall be provided either:
 - i. In paper form, which shall include any information that had been included via hyperlinks, or
 - ii. Electronically, via email, in accordance with the Privacy Practices – Patient Requests for Alternative Communications Policy (PP 1100).

Encryption: The PI, PEC or CRC shall encrypt the e-mail prior to sending the eIC to the Subject, which requires adding the word "encrypt" in the subject line of the e-mail. Patient Health Information should not be included in the subject line of the e-mail.

- b. The PI shall ensure that the Subject's signed eIC is filed and maintained in accordance with the Informed Consent Process for Research Studies Policy (BC-RES-105).

3. Security Controls

- a. If the eSIG is based on identification codes in combination with passwords:
 - i. The PI and/or staff working with the PI shall immediately notify the Electronic System administrator, if a report is received of any lost or stolen identification codes or password information.
 - ii. The Electronic System administrator shall then promptly deauthorize the identification code or password and issue a temporary or permanent replacement.

LEGAL REFERENCES

[FL Stat. § 668.50](#) – Uniform Electronic Transaction Act

[FL Stat. § 766.103](#) – Florida Medical Consent Law

[21 C.F.R. §§ 11 et seq.](#) – Electronic Records, Electronic Signatures, Food and Drug Administration (FDA) Regulations

[21 C.F.R. §§ 50 et seq.](#) – Protection of Human Subjects, FDA Regulations

[21 C.F.R. §§ 56 et seq.](#) – Institutional Review Board, FDA Regulations

[21 C.F.R. § 312.60](#) – General Responsibilities of Investigators re: Drugs for Human Use, FDA Regulations

[21 C.F.R. § 812.100](#) – General Responsibilities of Investigators re: Medical Devices, FDA Regulations

[45 C.F.R. §§ 46 et seq.](#) – Protection of Human Research Subjects, U.S. Department of Health & Human Services (HHS) Regulations

[45 C.F.R. § 164.312](#) – Technical Safeguards, HHS Regulations

[Use of Electronic Informed Consent: Questions and Answers](#), HHS, December 2016.

POLICY AND PROCEDURE REFERENCES

Informed Consent Process for Research Studies Policy (BC-RES-105), Exhibit B, including those policies referenced therein.

Privacy Practices - Patient Requests for Alternative Communications (PP 1100), Exhibit C

Electronic System User Guide, as referenced in Exhibit A [Insert link here].

EXHIBIT A
Electronic System Requirements For Electronic Informed Consent

Any eIC shall be obtained through the use of an Electronic System that satisfies the requirements detailed herein. BayCare shall confirm that the Electronic System is capable of satisfying these requirements. The Electronic System shall have a user guide to assist the authorized individuals to locate documentation. The vendor of the Electronic System shall certify that it and the Electronic System satisfy the applicable requirements of the HIPAA Privacy, Security, and Breach Notification Rules.

The Electronic System shall:

- Ensure that the person electronically signing the eIC is the Subject who will be participating in the study;
- Allow all versions of the eIC, including informational materials (e.g., weblinks, presentations), to be easily retrieved and printed upon the Subject or research team's request;
- Encrypt the Subject's information;
- Archive electronic documents appropriately;
- Limit system access to authorized individuals;
- Ensure that attempted use of an individual's eSIG by anyone other than its genuine owner requires collaboration of two or more individuals;
- Include the eSIG in any print out or electronic record;
- Indicate the printed name of the signer on the eIC, in addition to the date and time the signature was executed;
- Have the ability to allow the Subject to easily navigate the eIC;
- Allow the PI the ability to incorporate electronic strategies to encourage Subjects to access all of the consent material before documenting their consent, and shall allow the PI to include hyperlinks, if deemed necessary; and
- Ensure that the requirements for eSIGs are adhered to, as detailed below.

If the eSIG is based on identification codes in combination with passwords, the Electronic System shall use the following controls to ensure the security and integrity of the eSIGs:

- Maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password;
- Ensure that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging);
- Deauthorize any lost, stolen, missing, or otherwise potentially compromised identification codes or password information, and issue temporary or permanent replacements using suitable, rigorous controls;
- Use transaction safeguards to prevent unauthorized use of passwords and/or identification codes, to detect and report, in an immediate and urgent manner, any attempts of their unauthorized use to the PI; and
- Conduct initial and periodic testing of devices or generate identification codes or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Each eSIG shall:

- Link to its respective electronic record to ensure that it cannot be removed, copied, or otherwise transferred to falsify an electronic record;
- Only be able to be used by its genuine owner and not able to be reused by, or reassigned to, anyone else; and
- Employ at least two distinct identification components, such as an identification code and password.
 - When a Subject executes a series of signings during a single session of system access, the first eSIG shall be executed using both eSIG identification components; subsequent signings in the same session shall be executed using at least one eSIG component that is only executable by and designed to be used by that Subject.

- **When a Subject executes one or more signings not performed during a single, continuous session of system access, each signing shall be executed using both eSIG identification components.**