MCW Guidance: Reporting a Possible HIPAA Violation and/or Data Breach

In the event that a data or information was disclosed to an entity outside of the Medical College of Wisconsin that was not intended to receive Protected Health Information (PHI), the following process should be used:

1. Notify by e-mail both the IRB (irboffice@mcw.edu) and MCW Corporate Compliance (Matt Richter) of the event.
   a. The e-mail should include the following information when available:
      i. A description of the event including:
      ii. When the event occurred,
      iii. Who (name of) accessed/disclosed the PHI – Identify if FH employee or MCW employee,
      iv. What information was disclosed,
      v. To whom the information was disclosed,
      vi. Any outcome that is known at the time of the e-mail (i.e. recipient identified that the information was not intended to be sent and it was destroyed),
      vii. A unsigned consent form as an attachment,
      viii. If the recipient of the information is clearly called out in section E2 of the consent form either by name or contractual agreement it is also helpful to include that information in the e-mail.

2. The IRB, in conjunction with Corporate Compliance, will determine a) if a HIPAA breach has occurred and/or b) if a Reportable Event (RE) to the IRB is needed in accordance with the IRB SOP: *Requirements for Reporting to the IRB*. If it is determined that an RE is not required a copy of the response from IRB or Corporate Compliance and an internal deviation should be filed in the study file and reported to the IRB at the time of Continuing Progress Report (CPR). If it is determined that an RE is required the following steps should be followed.
   i. Open a RE submission for the research project in eBridge.
   ii. Upload the notification email to Corporate Compliance or document the phone call date, time, person making the call and who the information was reported to ensure that the immediate time frame is recorded.
   iii. Submit the RE to the IRB. At this time the IRB will review the attached information and send the RE back to the study team until final instructions are provided by Corporate Compliance.

3. Upon determination of a HIPAA breach, MCW Corporate Compliance will contact the study team with further instructions which may include notification to subjects (if needed). If the breach involved a Froedtert Health employee, MCW Corporate Compliance will copy FH OCRICC as their notification of the breach.
   i. In the event that the study team is instructed to notify subjects of a HIPAA breach, MCW Corporate Compliance will provide guidance on the content of the letter and will review the DRAFT notification letter.

4. After MCW Corporate Compliance approves the content of the notification letter:
   i. Upload the letter to the RE and submit to the IRB for review
   ii. IRB will review and either request changes or indicate that the study team should proceed with subject notification.

iii. Once a notification letter is approved by the IRB (with no changes) and the PI signs the letter, a PDF of the signed letter(s) must be e-mailed to MCW Corporate Compliance.
iv. If the IRB makes changes to the notification letter, it must be reviewed one final time by MCW Corporate Compliance. Once Final and the PI signs the letter(s), a PDF of the signed letter(s) must be e-mailed to MCW Corporate Compliance.

5. Proceed with subject notification and document this process in the RE and research project regulatory records/subject files, etc.

6. Re-submit the RE for IRB review

7. IRB will review the RE and request changes or acknowledge the RE