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

In the event that 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 Research Compliance, Ellen Manning (elmanning@mcw.edu) 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. An unsigned or redacted IRB approved 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. MCW Research Compliance, will determine if a HIPAA breach has occurred and the IRB will determine what level of reporting is required in accordance with the IRB SOP: *Requirements for Reporting to the IRB*.
   a. Events which do not meet MCW prompt reporting criteria should be reported to the IRB with a project's continuing progress report (CPR), a Reportable Event (RE) is not required. Include a copy of the response from the IRB and Research Compliance.
   b. Events which do meet MCW prompt reporting criteria should submit a RE.
      i. Open a RE submission for the research project in eBridge.
      ii. Upload the notification email to MCW Research Compliance to document the time frame for prompt reporting.
      iii. Submit the RE to the IRB. At this time the IRB will review the attached information and send the RE back to the research team until final instructions are provided by MCW Research Compliance.

3. Upon determination of a HIPAA breach, MCW Research Compliance will contact the research team with further instructions which may include notification to subjects. If the breach involved a Froedtert Health employee, MCW Research Compliance will copy FH Office of Clinical Research and Innovative Care Compliance (OCRICC) as their notification of the breach.
      i. In the event that the research team is instructed to notify subjects of a HIPAA breach, MCW Research Compliance will draft a notification letter and provide it to the Principal Investigator (PI) for review.

4. After MCW Research Compliance approves the content of the notification letter:
      i. The notification letter is signed by the PI, a PDF of the signed letter(s) must be e-mailed to MCW Research Compliance.
      ii. Upload the letter to the RE and submit to the IRB for review of the RE.

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