Email Containing PHI - Do's and Don'ts

Rule: Do	Guidance
Type the content of the email, attach documents, and review before including any email addresses.	Complete the email then decide who needs to receive it.
Use **"Secure:"** email Email must start with "Secure:" Not Re:, Fwd:, etc.	Any time you are sending PHI outside of the Commonwealth's firewall Email addresses ending in "mass.gov" and ". state.ma.us" are inside the firewall. **This encrypts the content of the email but not the subject line.**
Whether sending email within or outside the Commonwealth's firewall, use discreet subject lines that do **not** include PHI, such as "Personal and Confidential Communications."	Never put PHI, including pts initials in the subject line.
Make sure all state recipients have the intended agency initials at the end of their name to avoid sending emails to the wrong person.	Confirm state email addresses have agency initials at the end of the name (ex. (EHS) (DDS)(DYS)(DCF)). If the agency initials do not automatically appear; hover the cursor over the name and it will show.
Make sure all recipients outside of the state agencies have intended email address.	Confirm the business email address of all recipients outside of the state agencies (ex. @beaconhealthoptions.com; @acskids.org). [1] .
Verify identity and authority[2] of the individual or entity to which the information is to be disclosed. (See Chapter 11 of the Privacy Handbook.)	Document verification in the applicable Designated Record Set(s), using the mechanism for capturing disclosures for audit trail purposes, or directly on the applicable Authorization and/or written request for PHI.
Review and confirm both last and first name of the email recipient.	
Clean out/avoid using Autofill.	Delete all personal email addresses from Autofill.
Check any attachments are correct versions.	After attaching a document open it to confirm it's what you intend to send.
Avoid spreadsheets; convert to .pdfs.	Spreadsheets may contain pivot table that can reveal underlying PHI.
Limit any PHI in the body of email to what is necessary.	

[1] Contracted providers are required to comply with HIPAA and should not use personal email accounts, such as @gmail.com, @yahoo.com, etc.

[2] A client's written authorization to release PHI is authority to disclose.

Email Containing PHI - Do's and Don'ts

Rule: Do	Guidance
Include the DMH Confidentiality Notice.	Instructions on how to add this notice to your computer and state issued smartphone are in the attached PDFs. You cannot email PHI to or from your or any DMH Workforce Member's personal email account.
STOP and REVIEW: Before sending any email review the "To:" and "CC:" lines. Do you intend to send the email to each of the email addresses shown? Is the email being sent outside of the firewall? Properly using "Secure:"? Is there PHI in the subject line? Are attachments meant for all recipients?	Look at state agency abbreviations and all non-state agency addresses (.org; .com; .net; .gov) **You MUST Stop and Review**. This step takes you seconds. If skipped and an email error occurs, it takes DMH hours to address and may result in disciplinary action.

Rule: Do Not	Guidance
Do not email PHI.	Unless the disclosure is authorized and each recipient needs the information in order to perform their duties. As with any disclosure it should be the minimum necessary for them to perform their respective duties.
Do not copy PHI into emails if the recipient can directly access the source of the PHI.	Do not copy client records into an email if the recipient can directly access the client records.
Do not Use PHI in the subject line, including client names or initials.	Never put PHI, including pts initials in the subject line. Subject lines in emails are not encrypted! Even when using "Secure:" email. Chapters 3 and Chapter 6 of the Privacy Handbook prohibited use of patient initials.
Do not reply to or forward an email that contains PHI in the subject line.	Change the subject line before replying to or forwarding the email.
Do not send or reply with PHI to email distribution lists.	Unless you have confirmed each member of the group is an intended recipient.

Email Containing PHI - Do's and Don'ts

Rule: Do Not	Guidance
Do not "Reply to All" with emails containing PHI.	Unless you have confirmed each person is an intended recipient and that the information contained in the email is something that all persons on the distribution list need to know.[3]
Do not send email with PHI to a Gmail, Yahoo, or other individual email address.	Unless the identity and authority[4] of the individual or entity to which the information is to be disclosed has been verified.
Do not forward an email chain.	Unless the entire chain has been reviewed for PHI.
Do not create long email chains that contain PHI.	Edit, delete previous content no longer needed.
Do not Copy/Paste an email or email content into a client's medical record.	Information from an email should be summarized by the author of the note to prevent unintended and unnecessary information from being added to the client's medical record.

[3] DMH may rely on a Sender to have only included necessary recipients; however, if you see an email address that appears to be incorrect do not Reply to that address; delete it from your reply and separately send an email to the Sender noting that you believe the email address was not intended and that may be a privacy violation.

[4] A client's written authorization to release PHI is authority to disclose.