MedScribe Information Systems, Inc
HIPAA Policies and Procedures Articles

MedScribe HIPAA Statement:

MedScribe intends to protect the privacy and provide for the security of protected health information (PHI) in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA) and regulations promulgated by the U.S. Department of Health and Human Services.

POLICIES AND PROCEDURES

POLICY: HIPAA training and education.

PROCEDURE:

1. All staff, including independent contractors, will receive education regarding HIPAA and the protection of individually identifiable health information.
    a. HIPAA training will be included in orientation of new staff and/or independent contractors. Each individual will sign an attestation form verifying they have received this information.
    b. All staff, including independent contractors, will sign a confidentiality/nondisclosure form.

c. All staff, including independent contractors, will sign an attestation form verifying they have reviewed appropriate departmental policies and procedures.
d. New employees will sign an attestation form verifying they have received and reviewed the MedScribe Employee Handbook.

2. Ongoing HIPAA education will be provided through the following methods.
    a. Newsletter articles.
    b. Signs.
    c. Questions/answers in weekly self-assessment exercises.
    d. Reminder messages.
    e. Development of new policies and procedures.
    f. Presentations.
    g. Continuing education opportunities within professional organizations.

<u>POLICY</u>: Protected health information (PHI) as defined by HIPAA.

(PHI) as defined by HIPAA: Any information, whether oral or recorded in any form or medium, that (1) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse, and (2) relates to the past, present or future physical or mental health or condition of an individual, or the past, present, or future payment for the provision of health care to an individual.

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION AS DEFINED BY HIPPA

- Names
- Geographic subdivisions
- Dates (except year)
- Phone number
- Fax number
- E-mail address
- Web URLs
- IP (internet protocol)
- Social Security Number
- Medical record number

- Health plan number
- Account number
- Driving certificate/license number
- Vehicle identifiers/registration number
- Biometric identifiers
- Photographic images
- Device identifiers
- Other unique identifier

POLICY: Protection of documents that contain protected health information (PHI).

PROCEDURE:

1. Documents that contain PHI should be protected at all times from inappropriate access or viewing.
2. Immediately report to your supervisor any inappropriate access or viewing.
3. Do not leave documents with PHI on a shared printer or copy machine.
4. Do not leave documents with PHI on a computer screen while unattended.
5. Immediately report to your supervisor any security incident that may compromise PHI.
6. Do not discard documents with PHI in trash cans or waste bins.
    a. Place documents with PHI in designated containers for shredding.
    b. Discard documents with PHI by shredding.

POLICY: Home-based office and equipment.

- Safeguard the home office from unauthorized physical access, tampering, and theft.
- Report all security incidents immediately to your supervisor.
- Do not store or retain any PHI on computer system beyond the time the chart has been transcribed and transmitted to MedScribe.
- If it is necessary to print PHI, do not leave it on a printer for unauthorized individuals to view, and discard it by shredding.

- Maintain a current virus protection program to scan your computer system on a routine basis.
- Use firewall protection when connected to the Internet.
- Do not share your MedScribe password with unauthorized individuals.
- Do not remain logged-in when away from your workstation.
- Fax machines used for PHI must be located in secure areas and not accessible to unauthorized individuals. If faxing of PHI is required, use a cover sheet with the following disclaimer:

> The information contained in this facsimile message is privileged, confidential, and only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, please immediately notify us by telephone and return the original message to us at the address listed above via the US Postal Service. Thank you for your cooperation.

- Immediately report to your supervisor any inappropriate disclosure of PHI.
- Do not copy PHI on any storage media (i.e. floppy disks, CDs, etc.).
- At all times maintain and safeguard the confidentiality of PHI.

POLICY: Report of Wrongful Disclosures of PHI

PROCEDURE:

1. All employees or agents will immediately report any wrongful disclosure of PHI to their supervisor.
    a. Supervisors will immediately notify MedScribe's HIPAA Compliance Officer.
2. An investigation will be conducted to determine the following:
    a. What PHI was wrongfully disclosed.
    b. Where or to whom was the PHI disclosed.
    c. Who or what was responsible for this disclosure.
    d. Was this disclosure accidental or deliberate.
    e. What was the severity of damage caused by this disclosure.
    f. What was the cause for the disclosure.
    g. What procedures or training can be implemented to avoid similar disclosures in the future.
3. If it was determined that the employee or agent involved was not at fault for this wrongful disclosure, no sanctions will be applied.
4. If it was determined that the employee or agent was responsible for this wrongful disclosure, sanctions will be applied.

a. A MedScribe incident report will be filed by the immediate supervisor.
b. The individual will be counseled and educated regarding preventative measures to avoid similar disclosures in the future.
c. MedScribe's established progressive disciplinary action (as published in the Employee Handbook) will be followed unless the severity of the incident warrants additional sanctions or immediate termination.
    1. The established progressive disciplinary action includes:
        a. Oral warning
        b. Written warning
        c. Termination

5. The HIPAA Report of Disclosure form will be completed by MedScribe's Compliance Officer.
a. The information within this report will be reviewed by the supervisor to assure its accuracy.
b. The completed report will be sent by MedScribe's HIPAA Compliance Officer to the covered entity whose PHI was disclosed.

This report will be retained for 6 years in a file established by MedScribe's Compliance Officer.

<u>POLICY</u>: Sanctions for Wrongful Disclosure of PHI

PROCEDURE:

1. All employees or agents will immediately report any wrongful disclosure of PHI to their supervisor.
a. Supervisors will immediately notify MedScribe's HIPAA Compliance Officer.

2. An investigation will be conducted to determine the severity of damage caused by this wrongful disclosure and the individual responsible for the disclosure.
a. This investigation will be conducted by the immediate supervisor and MedScribe's Compliance Officer
b. If it was determined that the employee or agent involved was not at fault for this wrongful disclosure, no sanctions will be applied.

c. When the severity of the incident requires, the Director of Human Resources will be included in this investigation for the determination of applicable sanctions.

3. MedScribe's established progressive disciplinary action (as published in the Employee Handbook) will be followed unless the severity of the incident warrants additional sanctions or immediate termination.
   a. An incident report will be completed by the supervisor.
   b. The established progressive disciplinary action includes:
      1. Oral warning
      2. Written warning
      3. Termination
   c. The individual will be counseled by their supervisor.
   d. When the severity of the incident requires, the following disciplinary actions may include:
      1. Position demotion
      2. Position suspension
      3. Termination
   e. When termination has been deemed to be the appropriate sanction, the Director of Human Resources will conduct the termination process.

POLICY: Security of PHI with Email Communications

PROCEDURE:

1. When an email is received by the MedScribe office asking for protected health information (PHI), the MedScribe staff member will verify that the individual making the request is authorized to receive it in the following manner:
   a. Confirm the client name (the covered entity) and individual making the request from the email address used or information supplied within the email.
   b. Confirm that the individual's email address matches the email address listed in the client contact database located in Outlook Public Folders.
   c. If the individual's email address cannot be confirmed, the MedScribe staff member will call the client in order to verify that the individual making this request is at the client's location.
      i. The MedScribe staff member will dial the number recorded in our client contact database to call the individual making the request for PHI.

ii. If information regarding the individual requesting the PHI cannot be confirmed, PHI should not be released. Refer this request to MedScribe's Compliance Officer.
iii. The exception of this would only be on an emergent basis (see below under #4).

d. When responding to an email request, use reply to assure the email address is not keyed incorrectly.
    i. If any inappropriate PHI elements (i.e., patient's name, birth date, social security number, etc.) are used within the email by the sender, delete them so that the reply email does not contain this information. (See below under #3 for PHI elements that can be used within email communications.)

e. As a reminder, email sent from MedScribe's email server will automatically have the pre-approved confidentiality statement included in it.

f. When any email that contains PHI is printed, it should not be discarded in the trash; it must be placed in the shred box.

g. The MedScribe staff member will not provide PHI to a third party. Only individuals from the covered entity where the dictation (report) was originated, the dictator and those copied on it, are authorized to receive it.
    i. The exception of this would only be on an emergent basis (see below under #4).

2. Never email a report (or chart) as either an attachment or pasted within the body of the email.
    a. Send reports through the usual established secure method used for chart delivery for that client.
    b. If the usual established secure method is not available, the report can be faxed. Refer to the Security of PHI with Fax Requests policy.
    c. The exception of this would only be on an emergent basis (see below under #4).
3. Limit the use of PHI within an email in the following manner.
    a. Never use the patient's name in the email.
    b. Do not use any PHI within the reference or subject line.
    c. Limit the identifying information to use of any of the following items:
        i. Dictation voice file number.
        ii. Job number.
        iii. Medical record number.
        iv. Account number.

v. Date dictated and/or date transcribed.
vi. Physician(s) name(s).

4. In the case of an emergency, MedScribe will support HIPAA's "break the glass" rule by immediately providing the PHI requested in order to assure patient care is not impeded by the delay of providing PHI required on an emergent basis.
    a. The MedScribe staff member will notify MedScribe's Compliance Officer in writing of any incident that requires PHI to be provided on an emergent basis.

MedScribe's Compliance Officer will follow up with the covered entity to assure that no inappropriate release of PHI had occurred in responding to the emergent request.

POLICY: Security of PHI with Telephone Calls

PROCEDURE:

1. When an individual calls the MedScribe office asking for protected health information (PHI), the MedScribe staff member will verify the caller is authorized to receive the information requested in the following manner:
    a. Confirm the name and staff position of the caller, and confirm the client's name (the covered entity) and its geographic location.
    b. This contact information will be verified within the client contact database.
    c. If the contact information cannot be confirmed, the MedScribe staff member will do a call-back procedure in order to verify that this individual is at the client's location.
        i. For the call-back procedure, the MedScribe staff member will tell the caller that they will call them back.
        ii. Then the MedScribe staff member will dial the number recorded in our client contact database to call that individual back.
        iii. If information regarding the caller cannot be confirmed, PHI should not be released. Refer this request to MedScribe's Compliance Officer.
        iv. The exception of this would only be on an emergent basis (see below under #2).
    d. When the phone call is to request a report (or chart), do so in the following manner.

i. Send the report through the usual established secure method used for chart delivery for that client.
ii. If the usual established secure method is not available, the report can be faxed. Refer to the Security of PHI with Fax Requests policy.
iii. Never email a report as either an attachment or pasted within the body of the email.
iv. The exception of this would be only on an emergent basis (see below under #2).

e. The MedScribe staff member will not provide PHI to a third party. Only individuals from the covered entity where the dictation (report) was originated, the dictator and those copied on it, are authorized to receive it.
    i. The exception of this would only be on an emergent basis (see below under #2).

2. In the case of an emergency, MedScribe will support HIPAA's "break the glass" rule by immediately providing the PHI requested in order to assure patient care is not impeded by the delay of providing PHI required on an emergent basis.
    a. The MedScribe staff member will notify MedScribe's Compliance Officer in writing of any incident that requires PHI to be provided on an emergent basis.

MedScribe's Compliance Officer will follow up with the covered entity to assure that no inappropriate release of PHI had occurred in responding to the emergent request.

POLICY: Security of PHI with Fax Requests

1. When a fax is received by the MedScribe office asking for protected health information (PHI), the MedScribe staff member will verify that the individual making the request is authorized to receive it in the following manner:
    a. Confirm the client name (the covered entity) from the client's faxed coversheet form and its identifying fax number (printed on the top margin of the received fax sheet).
    b. Confirm that the fax number provided on the faxed coversheet matches the fax number listed in the client contact database located in Outlook Public Folders.
    c. If the fax number cannot be confirmed, the MedScribe staff member will call the client in order to verify that the individual making this request is at the client's location.

i. The MedScribe staff member will dial the number recorded in our client contact database to call the individual making the request for PHI.
ii. If information regarding the individual requesting the PHI cannot be confirmed, PHI should not be released. Refer this request to MedScribe's Compliance Officer.
iii. The exception of this would only be on an emergent basis (see below under #2).

d. When the fax is to request a report (or chart), do so in the following manner.
    i. Send the report through the usual established secure method used for chart delivery for that client.
    ii. If the usual established secure method is not available, or if fax was specifically requested, the report can then be faxed.
    iii. Never email a report as either an attachment or pasted within the body of the email.
    iv. The exception of this would be only on an emergent basis (see below under #2).
e. When faxing, verify the fax number is correctly keyed.
f. When faxing, use the MedScribe fax coversheet that includes the pre-approved confidentiality statement
g. When the faxing has been completed, place all materials with PHI in the shred box. Do not discard materials with PHI in the trash.
h. The MedScribe staff member will not provide PHI to a third party. Only individuals from the covered entity where the dictation (report) was originated, the dictator and those copied on it, are authorized to receive it.
    i. The exception of this would only be on an emergent basis (see below under #2).

2. In the case of an emergency, MedScribe will support HIPAA's "break the glass" rule by immediately providing the PHI requested in order to assure patient care is not impeded by the delay of providing PHI required on an emergent basis.
    a. The MedScribe staff member will notify MedScribe's Compliance Officer in writing of any incident that requires PHI to be provided on an emergent basis.
    b. MedScribe's Compliance Officer will follow up with the covered entity to assure that no inappropriate release of PHI had occurred in responding to the emergent request.

"After reading these articles, complete and return the HIPAA Confirmation Form"