



Providence Health & Services

The 1st HIPAA Fine & Resolution Agreement

(A Note to the Reader - The information contained in this document is meant for informational purposes only and not intended to act as a substitute for the advice of an attorney. Please contact appropriate legal counsel before acting on any of the information contained in this document.)

The first ever HIPAA fine and “Corrective Action Plan” has been levied against a non-profit hospital system with operations in multiple locations. Since 2003, many organizations that have experienced massive breaches of Protected Health Information (PHI) have not been “pulled over” by the “HIPAA police” and none received fine. That situation has changed dramatically with the latest enforcement action.

Providence Health and Services (PH&S) is the first hospital chain to be fined under the HIPAA Privacy and Security rules. PH&S entered into a Resolution Agreement (Agreement) with the Department of Health and Human Services (HHS) and has agreed to fulfill the terms of a “Corrective Action Plan” (CAP) and will pay a fine of one hundred thousand dollars.

The terms of the Resolution Agreement will be summarized in this document. The purpose of this update is to alert healthcare providers about the consequences if they are audited by HHS or the Office of the Inspector General (OIG).

Providence was fined for leaving disks, tapes, and laptops containing unencrypted PHI unattended and, in several instances, equipment containing PHI was lost or stolen between September 2005 and March 2006. The covered entities (CEs) fined and subject to the Resolution Agreement are PH&S in Washington, Providence Health Systems in Oregon (PHS), Providence Home and Community Services (a division of PHS or HCS) and Providence Hospice and Home Care (PHHC), also in Washington.

A summary of the terms of the Resolution Agreement are as follows:

- 1) The CEs agree to pay a fine of \$100,000.00 dollars by certified check to HHS.
- 2) The CEs must comply with the terms of a Corrective Action Plan or CAP. If any single CE breaches the CAP, then all CEs will be considered to be in violation of the Resolution Agreement and HHS will not be subject to the terms and conditions in the “Release” portion of the Agreement.
- 3) The release portion of the Agreement does not prevent the federal government from criminally prosecuting employees at PH&S.



- 4) The CEs cannot contest any fine or any additional fine that arises under this Agreement.
- 5) The Agreement and information related to the Agreement can be disclosed and falls under the Freedom of Information Act.
- 6) The CAP lasts for three years.
- 7) The CEs must submit written policies and procedures to HHS mentioned in the CAP and as required by the Privacy and Security rules.
- 8) Within specified time frames mandated in the CAP, the CEs must provide their policies and procedures to HHS for review and edits. The CEs must incorporate these changes into their policies and procedures.
- 9) Within a specified timeframe the CEs must implement these policies and procedures throughout their organizations. The CEs must show proof of that implementation or documentation of the implementation.
- 10) Within a specified timeframe, the CEs must distribute the policies and procedures to all members of their workforces that have access to ePHI. The CEs must document this distribution or be able to show proof.
- 11) The CEs must provide all new work force members with these policies and procedures.
- 12) The CEs must obtain from each workforce member a signed written or electronic compliance certification that each work force member has read, understands and will abide by the policies and procedures.
- 13) The CEs must revise these policies and procedures at least yearly or more often as required. These new policies and procedures will also be reviewed and edited by HHS. The CEs must distribute these updated policies and procedures to all workforce members and obtain a new compliance certification from each employee that deals with ePHI.
- 14) In addition to the following policies and procedures, the CEs must have any others as required by the Privacy and Security rules. At a minimum the CEs must have the following policies and procedures:

“The conduct of a risk assessment of potential risks and vulnerabilities to confidentiality, integrity and availability of ePHI when it is created, received, maintained, used or transmitted off-site;



The conduct of a risk management plan that implements security measures sufficient to reduce risks and vulnerabilities identified by the risk assessment to a reasonable and appropriate level;

Physical safeguards governing the off-site storage of backup electronic media containing ePHI;

Physical safeguards governing the off-site transport of backup electronic media containing ePHI;

Physical safeguards governing the physical security of portable devices containing ePHI;

Technical safeguards governing encryption of backup electronic media containing ePHI;

Technical safeguards governing encryption of portable devices containing ePHI;

Other technical safeguards governing backup electronic media containing ePHI (e.g., password protection);

Other technical safeguards governing portable devices containing ePHI (e.g., password protection)."¹

- 15) Within a specified timeframe in the Agreement, if the CEs determine that a workforce member has violated a policy or procedure they must notify HHs within 30 days of discovering this violation. This is known as a "Reportable Event."
- 16) The Reportable Event or RE must contain a compliance description of the event, the employees or persons involved, and the parts of the policies and procedures involved.
- 17) In addition, the RE must include a description of the CEs actions taken to mitigate this breach and any other information the CE will take to prevent this type of an action from occurring again.
- 18) Within a specified timeframe, the CEs shall provide evidence that they have provided training to all workforce members who have access to ePHI. All new members of the workforce must be trained as well.

¹ <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>



- 19) Each member of the CEs' workforce that receives training must obtain a written or electronic certification of training. The CEs must review training annually.
- 20) Workforce members that are not trained and certified, cannot access ePHI in offsite storage, transport of backup media containing ePHI, or the transport of portable devices containing ePHI.
- 21) The Chief Information Security Officer or CISO of PH&S shall conduct "Monitor Reviews" of all CEs to validate the following:

"All members of the HCS and PHHC workforce are familiar with the Policies and Procedures;

All members of the HCS and PHHC workforce are complying with the Policies and Procedures;

All backup electronic media related to HCS and PHHC containing ePHI are created and secured in compliance with the Policies and Procedures; and

All portable devices, regardless of type (e.g., laptop, Blackberry, personal digital assistant, etc.) or ownership, that contain ePHI and are under the control of members of the HCS and PHHC workforce, satisfy all applicable requirements of the Policies and Procedures."²

- 22) The unannounced Monitor reviews must include at a minimum, but not limited to the following:

"Unannounced site visits to HCS and PHHC facilities;

Interviews with a random sample of members of the HCS and PHHC workforce who use portable devices;

Interviews with members of the HCS and PHHC workforce involved in the supervision, use, retention, or destruction of, backup electronic media; and

Inspection of a random sample of portable devices that contain ePHI and are under the control of members of the HCS and PHHC workforce to ensure that such devices satisfy all applicable requirements of the Policies and Procedures."³

² <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>

³ <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>



23) The CE shall conduct these Monitor Reviews on a quarterly basis for the term of the CAP or three years. Based upon the results of these reviews PH&S shall:

“Identify any risks to the confidentiality, integrity, and availability of ePHI residing on backup electronic media or portable devices;

Develop recommendations to reduce such risks or vulnerabilities to a reasonable and appropriate level; and

Ensure that Covered Entities implement such risk managements steps.”⁴

24) The CEs must comply with all portions of section 45 CFR § 1664.308(a) (ii) (B).

25) The Monitor Reviews must be documented and include at a minimum the following:

“Dates of unannounced site visits;

Summaries of results of interviews;

Summaries of inspections of portable devices;

Descriptions of any risks identified; and

Any recommendations to reduce such risks.”⁵

26) Within 120 days of HHS’s approval of the policies and procedures PH&S’s CISO must submit a written report to HHS summarizing the CEs implementation of the CAP. This Implementation Report must include the following:

“An attestation signed by PH&S’s CISO attesting that the Policies and Procedures are being implemented, have been distributed to all members of the HCS and PHHC workforce and all members of the PH&S workforce who have access to the ePHI of HCS or PHHC, and that Covered Entities have obtained all of the compliance certifications required by sections VI.B.2. and VI.B.3. of the Resolution Agreement.

⁴ <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>

⁵ <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>



A copy of all training materials used for the training required by this CAP, a description of the training, including a summary of the topics covered, the length of the session(s), and a schedule of when the training session(s) were held;

An attestation signed by PH&S's CISO attesting that all members of the HCS and PHHC workforce, and all members of the PH&S workforce who have access to the ePHI of HCS or PHHC, have completed the training required by section VI.D. and have executed the training certifications required by section VI.D.2. of the Resolution Agreement.

An attestation signed by PH&S's CISO listing all HCS and PHHC locations (including mailing addresses), the name under which each location is doing business, the corresponding phone numbers and fax numbers, and attesting that each location is in compliance with the obligations of this CAP; and

An attestation signed by PH&S's CISO stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.”⁶

27) PH&S’s CISO must submit an Annual Report that reflects the CE’s status in complying with the CAP that contains the following information:

“A copy of the schedule, topic outline, and materials for the training programs provided during the Reporting Period that is the subject of the report;

An attestation signed by PH&S's CISO attesting that Covered Entities obtain and maintain written or electronic training certifications from all persons that must attend training, and that such training complies with the requirements established under this CAP;

A summary of Reportable Events (defined in section VI.C.10.) that occurred during the Reporting Period and the status of any corrective and preventative action(s) relating to all such Reportable Events;

A copy of reports generated by Monitor Reviews pursuant to section VI.E.5. and

An attestation signed by PH&S's CISO attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.”⁷

⁶ <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>



28) Finally, if the CEs breach this resolution Agreement and do not remedy that breach within 30 days, HHS will be able to impose Civil Money Penalties⁷ on the CEs for *“any violations of the Privacy and Security Rules related to the Covered Incidents set forth in paragraph 2 of the Resolution Agreement and for any other act or failure to act that constitutes a violation of the Privacy or Security Rules. HHS shall notify Covered Entities in writing of its determination to proceed with the imposition of a CMP.”*

⁷ <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>