

HIMSS

Electronic Personal Health Records (ePHR) Checklist

This checklist is provided to assist in the evaluation of a PHR against HIMSS' established definition and recommended features and functionality. If you have any questions about this checklist, please refer to the HIMSS PHR Definition (http://himss.org/ASP/topics_phr.asp) or direct questions to contacts on http://himss.org/ASP/topics_phr_committees.asp?faid=183&tid=34.

ePHR Provider/Vendor

One or more of the following may be checked.

- Obtained from patient's healthcare provider(s).
- Obtained from patient's employer.
- Obtained from patient's health plan.
- Obtained from the government.
- Obtained from an Internet site.
- Obtained from patient's pharmacy.
- Obtained from a disease management vendor engaged with the patient.
- Obtained from a device manufacturer.

Content Entry

One of the following must be checked.

- Untethered/Disconnected* content model: ePHR content is the result of direct entry from the patient or his or her legal proxy(s).

OR

- Tethered/Connected* content model: An internet portal that receives data from one organization that participates in the individual's healthcare, such as an institutional EMR/EHR or health insurance claims database. Allows patients or proxies to enter their own data (such as journals and diaries). The institution that provides the ePHR owns and manages the ePHR, allowing patient access.

OR

- Interoperable* content model: An internet portal that receives data from multiple constituents that participate in the individual's healthcare, such as pharmacies, hospitals, health insurers, etc. Allows patients or proxies to enter their own data (such as journals and diaries).
 - *Federated*: The ePHR contains pointers to data on the various constituents' databases.
 - *Central database*: Data from various constituents is copied to a central database for viewing within the ePHR.

Security and Access Features

All of the following must be checked to comply with HIMSS' recommendations.

- Unique patient identification.
- Owned, managed and shared by the individual or his or her legal proxy(s).
- Allows secure access to the information contained in the ePHR.
- Allows designation of information to be shared electronically with the patient's consent.
- Permits the receipt of email alerts that do not reveal protected health information (PHI).
- Permits the designation of information to be shared electronically.
- Has ability to designate read-only access to the ePHR (or designated portions thereof).
- Provides technical support to ePHR constituents at all times.
- Allows consumers to export data from their ePHR (portable).
- Allows providers, with patient/proxy consent, to export data out of ePHRs or mine data from ePHRs for legitimately defined purposes, such as population health research or health trend analysis.
- Provides log of both information shared and information recorded (or entered into the ePHR), including an audit trail of who has entered, accessed, or modified the information.
- Provides access to the privacy policy of the source or offerer of the ePHR.