Personal Health Record Report Card

Report Card for CapMed – icePHR

This PHR is primarily for use "in case of an emergency" www.icephr.com	A	B	C	D	F	GRADE = C *(See Below for Grade Explanations)*
Privacy Policy/Notice:						
• Location: Privacy Policy must be easy to find and accessible from the organization's home page. Should be unavoidable and accessible on any page that collects information.				✓		Privacy Policy is found at the bottom left corner, small link. It is item 6 of 13 in a comprehensive legal document.
• Readability: Privacy Policy must be clear, easy to understand, and at a low reading level.				✓		Written by lawyers, for lawyers. Very few declarative statements at a very high reading level. The Disclaimer of Warranties and Limitations of Liability written in all BOLD conveys a "get out of jail free" card for the company rather than any meaningful commitment to privacy or security. None of their policy invokes much confidence in protecting privacy. We don't get the sense this policy is meant to really inform or engage the user.
• Transparency: Privacy Policy is comprehensive; individuals should not have to read multiple policies to understand how their information can be used.			✓			Privacy Policy is part of long legal agreement (13 pages) and refers to other components of the legal agreement, including the Disclaimer/Limits of Liability referenced above. The reference to HIPAA compliance is confusing and unclear. Does this mean CapMed will use any health information without getting your consent if it's for "treatment, payment or healthcare operations"?
Patient Control/Choice:						
• Consent for Identifiable Data: No information is shared or collected without explicit, informed consent. Privacy Policy states how information will be shared and, ideally, how it will NOT be shared.			✓			CapMed states they will not share individual patient information "*during the registration process*" with third parties, "*including health insurers.*" It's a good sign that they explicitly commit to not share with insurance companies. However, they also state they are in full compliance with HIPAA as a non-covered entity. This provides us no assurance, as HIPAA allows sharing without consent for "treatment, payment, and healthcare operations." It is difficult to tell based soley on this policy, but the reference to HIPAA opens a huge loophole. Also, is information provided 'during registration' the only information protected? Of note, if the company is sold or merged, your information will be shared with the "*actual or prospective purchasers*". As it's written, it would not appear that they would need to get your permission to share all your identifiable data if the company goes bankrupt and they are bought out by an insurance company, marketing company or researcher.

						Finally, CapMed never quite commits to holding 3rd parties accountable. "*CapMed **may** undertake efforts to see that any third party… is under contractual obligation to use the information solely for the purpose for which the information was disclosed… CapMed is not responsible for... their conduct...*" If a company can't commit to at least contractual requirements, why should anyone trust them with their personal data?
• "De-Identified Data": No de-identified or aggregate data should be used without explicit, informed individual consent.					✓	Shares "de-identified" data, no opt out.
• Segmentation: Patients can segment/hide sensitive information.		✓				You have the ability to hide each condition, medication, immunization, etc. to Emergency personnel (ER access is the primary feature of this PHR). Can share with HealthVault but all information is copied, doesn't appear to allow segmentation there.
Access/Participation:						
• Patients can easily find out who has accessed or used their information.		✓				You receive an email when someone accesses information with the reason for accessing. You can also see a history of access.
• Patients must be able to promptly and permanently remove themselves and their health information from the system upon request.			✓			You are able to delete any/all information. You must email customer service and it will be deleted in three (3) business days. No mention of any permanent files or if they retain the records internally for any period of time after patient requests deletion.
Integrity/Security:						
• Patients can expect their data to be secure. Data should only be stored in the U.S. and use authentication that goes beyond username and password login.				✓		From the Disclaimer of Warranties and Limitations of Liability: No warranty that any content "*will remain unaltered, uncorrupted and unusable…secure from attack…*" They do maintain encryption, firewalls, compliant with HIPAA security requirements. No mention of whether or not the data is stored in the U.S.
Customer Service/Enforcement:						
• Patients can easily report concerns and get answers.				✓		Email, mail and 800# available for customer support. Sent an email on 11/10/09 and as of 12/01/09 had not received a response.

View CapMed's entire Privacy Policy. We highlighted sections of importance.
www.patientprivacyrights.org/CapMed_Privacy_Policy

Letter Grade	Numerical Value	Explanation
A	4.0 - 5.0	Excellent: No invasive practices; solid protections; ensures your privacy rights; user friendly.
B	3.1 - 3.9	Fairly comprehensive efforts and protections, room for improvement
C	2.6 - 3.0	Some safeguards, a number of key flaws, weak protections
D	2.0 - 2.5	Few, if any, safeguards and protections, and/or misleading information, and/or very user "un-friendly."
F	1.0 - 1.9	Threatens patient privacy and control over personal information either via inaction or actual business practices

CapMed's Numerical Grade:
2.6