TESTIMONY OF LEGACY HEALTH

REGARDING SENATE BILL 601

Legacy Health operates six hospitals and more than 20 outpatient clinics in metropolitan Portland. Legacy Health is Oregon's largest non-insurance affiliated hospital system.

The concerns of Legacy Health and other hospitals regarding SB 601 relate to the proposed expansion in the definition of "personal information to include information that is currently protected under the provisions of the Health Insurance Portability and Accountability Act of 1996, commonly known as "HIPAA." Under the dash 2 amendments, the following additional categories of information would be added to Oregon's Consumer Identity Theft Protection Act:

> "(F) A consumer's health insurance policy number or subscriber identification number in combination with any other unique identifier that an insurer uses to identify the consumer; or "
>
> "(G) Any information about a consumer's mental or physical condition, medical history or medical diagnosis or treatment. " *See SB 601-2, page 1, lines 8 – 12.*
>
> These are the very kinds of information covered by HIPAA.

HIPAA is enforced by the Office for Civil Rights of the US Department of Health and Human Services. That agency has promulgated the "HIPAA Privacy Rule," which protects the privacy of individually identifiable health information; the "HIPAA Security Rule," which sets national standards for the security of electronic protected health information; the "HIPAA Breach Notification Rule," which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the "Patient Safety Rule," which protect identifiable information being used to analyze patient safety events and improve patient safety.

Oregon's Consumer Identity Theft Protection Act already has an exemption for HIPAA compliant entities from the requirements to develop safeguards for personal information. *ORS 646A622 (2)(c).* But because the kinds of personal information defined in (F) and (G) above were not included in the Act as written in 2007, the Act does not include an exemption for HIPPA compliant entities from provisions

requiring notice to consumers and others of a breach involving health insurance or medical information. *Compare 646A.604(8).* If these additional types of "personal information" are added to the Act now, a HIPPA compliance exemption is necessary to avoid hospitals and other entities subject to HIPAA from inconsistent notification requirements, thresholds and timelines.

The HIPAA breach notification requirements and timelines are summarized in the attachment to this testimony, taken directly from the website of the Office of Civil Rights. There is no threshold for notice under HIPAA, in contrast to that proposed in SB 601. The requirements for notice, both in terms of the method of giving notice, timelines for doing so, and parties entitled to notice, are also considerably different than those in the Act as modified by SB 601.

For these reasons, because the Act already recognizes that health insurance and medical information is adequately protected under HIPAA, and due to the different breach notification requirements under HIPAA, we request that SB 601 be amended to include a HIPAA compliance exemption to the notification requirements of the Act contained in ORS 646A.604.

Respectfully submitted,

Paul Cosgrove 503-799-5679

pcosgrove@lindsayhart.com

Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Definition of Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

There are three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Unsecured Protected Health Information and Guidance

Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

This guidance was first issued in April 2009 with a request for public comment. The guidance was reissued after consideration of public comment received and specifies encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Additionally, the guidance also applies to unsecured personal health record identifiable health information under the FTC regulations. Covered entities and business associates, as well as entities regulated by the FTC regulations, that secure information as specified by the guidance are relieved from providing notifications following the breach of such information.

Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

- **Individual Notice**

  Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

  These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

- **Media Notice**

  Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- **Notice to the Secretary**

  In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html) and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

- **Notification by a Business Associate**

  If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

Administrative Requirements and Burden of Proof

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or

disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.