Dear Randi,

Thank you for your thoughtful letter about inBloom. We appreciated the advice you provided in the early stages of development of the Shared Learning Collaborative, whose mission is now being carried forward by inBloom, and equally welcome this continued dialogue as we move forward. Your concerns are addressed in detail below. As initial funders we take these seriously, and would therefore be happy to make your letter and our response public, as we are working hard with inBloom to set the record straight and communicate the value it can bring to so many students and educators. To that end, we would be happy to set up a meeting when all of us could sit down with inBloom's leadership to further discuss your concerns.

Issues of data privacy and security for both teachers and students are of the utmost importance to inBloom, and that is why, since the early design phase, it has continually sought advice from some of the leading experts in the field to ensure that it would exceed existing requirements and deliver a more secure service to states and districts than the systems they currently have in place.

As you know well, for years, states and school districts have been independently collecting and maintaining student data required for teachers to do their jobs effectively; however, this data is often housed in costly, outdated systems that take too much time away from teaching.

At the same time, to succeed in today's world, students need learning experiences that meet their specific needs, engage them deeply, and let them learn at a pace that meets their individual requirements. That's why teachers, parents, and education advocates believe that in order to raise achievement, personalized learning needs to become a reality for every student. With the right technology in place, schools can extend the reach and effectiveness of teachers so that more students get what they need, when they need it, at scale and in a cost-effective way.

Inspired by the vision of the Council of Chief State School Officers (CCSSO) and in interest from states and districts, inBloom is a new resource that helps teachers better manage and use the same secure data that states and districts have collected for years. Once it is fully operational, inBloom will make it easier for teachers, parents and students to be more involved and informed, track student progress and make learning more engaging for students. While it offers many rich benefits, inBloom helps to address complex challenges with a technical solution – that works behind the scenes like plumbing – that has never been seen before, and as a result, inBloom is more vulnerable to mischaracterizations.

We all know that change is difficult, often controversial, and it takes time and continued commitment. As you note, inBloom needs to do more work to explain how it can help teachers improve and personalize learning for all students. To that end, we will advise inBloom to continue to encourage participating states and districts to ensure public engagement and transparency on these important topics by:

1. Hosting public forums in states that have engaged with inBloom to address community concerns.

2. Creating policy committees – including practicing teachers – to develop guidelines and best practices regarding student and teacher data.

Below are detailed responses to your questions:

- **What are inBloom's plans to charge states for use of its cloud-based data repository?**
    - Beginning in 2015, inBloom's current pilot states and districts will pay an annual fee of no more than $5 per student, but will be as low as $2 per student over time.
    - New districts from pilot states will be able to use the service for free until 2015.
    - New districts from non-pilot states will begin to pay fees immediately.
    - Over time, as inBloom scales, the goal is to pass on fixed cost savings to users and ultimately reduce the cost of the per-student fees.

- **What are inBloom's plans to charge vendors for access to student data? What is the level of disaggregation of the data vendors have access to? Can vendors access personally identifiable information?**
    - Charging vendors:
        - inBloom does not sell student data to vendors. Rather, states and districts choose which vendors to use and contract with those vendors directly, just as they always have.
        - As a non-profit organization, inBloom is exploring cost recovery partnerships with select vendors, which are contracted by states and districts, for the services that it provides. These recovered costs will ultimately be passed on to participating districts through lower annual fees.
    - Disaggregation of data:
        - Students and teachers need data-rich applications to support personalized learning at scale.
        - Each application a district implements has different data requirements. inBloom allows districts to launch those applications more cost effectively, efficiently and securely than ever before with a time saving single sign-on portal for the teachers.
        - Many applications require student and classroom-level enrollment and achievement information to help a teacher answer the central question "How my students are doing and what might I do next to help them succeed?"
    - Vendor access to student data:
        - Participating states and districts decide what data will be collected and stored through inBloom, and the states and districts maintain control over that data at all times.
        - Participating states and districts also determine which vendors they will use, which applications they need from those vendors, and what data those applications require.
        - inBloom does not and will never sell any student data to anyone.

- **How is inBloom assuring that there is no unauthorized access to personally identifiable data? How is authorized data determined at vendor, state, district, and school levels? What additional privacy limitations does inBloom plan to attach to data beyond the differing limitations applied by states and districts?**
    - Each participating state or district will have its own protected data storage space, and will continue to own, manage and control access to its data, just as it always has.
    - Since its inception, inBloom has been advised by some of the leading legal, digital privacy and security experts in the country to help keep the data stored by states and districts secure. These include:
        - Shawn Henry, President of Services, CrowdStrike; Former Executive Assistant Director for cyber investigations at the FBI
        - Jay Pfeiffer, Senior Associate, MPR Associates, Inc.; Former Deputy Commissioner for Accountability, Research, and Measurement, Florida Department of Education
        - Christopher Wolf, Director at Hogan Lovells LLP's Privacy and Information Management Practice; Founder and Co-chair of the Future of Privacy Forum
        - Michael Gibbons, managing director with advisory firm Alvarez & Marsal, who spent 15 years with the FBI's Computer Investigations Unit where he oversaw all cybercrime investigations.
    - inBloom continues to work closely with these advisors and continues to review its policies and procedures in order to maintain best in class security and privacy systems and practices.
    - inBloom does not and will not accept social security numbers (SSNs) as unique student identifiers.
        - In the past, inBloom's policy has been to prohibit the storage and use of SSNs as a unique identifier unless the state or district applied for a waiver to that policy.
        - No such waivers were ever issued, and going forward inBloom will prohibit the use of SSNs under any circumstances and will not offer waivers.

- **Among dozens of pages of potential data fields are specific health and disability data that, in other uses, would require specific parental consent for access under the HIPPA regulations. How is that being addressed?**
    - inBloom does not facilitate the collection of any data not already collected by the states and districts; it simply helps states and districts manage the data in a more secure and cost-effective way to power learning applications that teachers need.
    - inBloom uses existing data standards that allow districts and states to manage information under their own local policies, in keeping with FERPA and the federal government's joint guidance on FERPA and HIPPA.
    - Also of note, recent changes to FERPA did not affect the kind of services inBloom provides to states and districts, and inBloom will conform to whatever FERPA requires.

- **What is the current implementation status of the Phase I pilot states? What is planned for Phase II, and what states have committed to participation?**
    - The use of “Phase 1” and “Phase 2” terminology was confusing and inBloom is no longer using that terminology.
    - To clarify:
        - Currently, New York, Massachusetts, Colorado, North Carolina, and Illinois are working with inBloom. Pilot districts in New York, Colorado and Illinois are working to evaluate inBloom’s offerings, and each is at a different stage in discussions and implementation timelines.
        - Georgia, Kentucky, and Delaware continue to be observers to assess the benefits that inBloom can bring to their states and districts by making available to teachers tools that are customized to the needs of their students.
        - Louisiana initiated activity with inBloom but stopped implementation to discuss its plans with various community stakeholders. Currently there is no data from Louisiana on inBloom’s system, but inBloom continues to engage in discussions with Louisiana education officials.

- **Some experts have expressed concern over cloud-based storage of sensitive data. How secure is this approach compared with other methods?**
    - States and districts already maintain many systems that contain student data, many of which are internet or cloud-based. This data is necessary to effectively operate schools, but it's often housed in costly, outdated and less secure systems that make it difficult for teachers, districts, and states to do their jobs.
    - Through inBloom, student data is stored in a secure, cloud-based data repository, and the security measures used by inBloom to protect that data exceed the security measures in place currently in most states and school districts.
        - inBloom uses Amazon Web Services, known as AWS, as its cloud service provider. AWS is one of a handful of services that is fully certified through the new FedRAMP program, a federal government procurement program that sets stringent standards that a cloud service must meet to be considered secure.
        - A recent study of more than 1,800 organizations found that on-site data environments are about 3 times more likely than cloud environments to be attacked by malicious software. (Alert Logic Report “Targeted Attacks and Opportunistic Hacks: State of Cloud Security Report” Spring 2013)

- **Much attention has been rightly focused on student data, and little has been said about personally-identifiable teacher data in relation to student characteristics and performance. The same concerns outlined above about access, sale and authorized use are relevant to teacher data, with the added issues related to evaluation and licensure and reciprocity.**
    - As with student information, school districts decide what teacher information is collected and stored, who has access to it, and how it is utilized. No data of any kind is shared across states or districts.
    - To be clear, inBloom has no ownership of student or teacher records whatsoever and will never sell it to anyone.

Again, we appreciate the chance to respond to your questions and concerns and look forward to continuing an open dialogue.

Sincerely,

Michele Cahill
Vice President, National Program
Carnegie Corporation of New York

Stacey Childress
Deputy Director, Innovation
Bill & Melinda Gates Foundation